Gigabit Web Smart Switch

User's Manual

Rev. 1.21c-EV

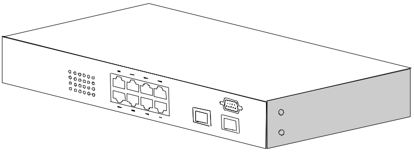
We make no warranties with respect to this documentation and disclaim any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. We reserve the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

About this manual …

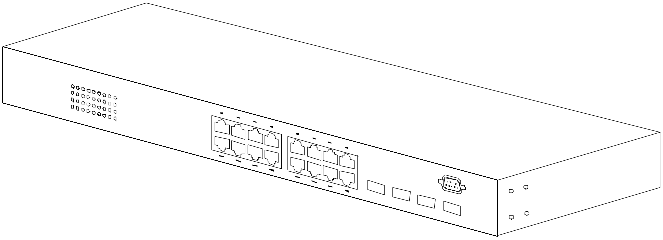
This manual is a general manual for different models of our Gigabit Web Smart Switch. They are similar in operation but have different hardware configurations.

These models are

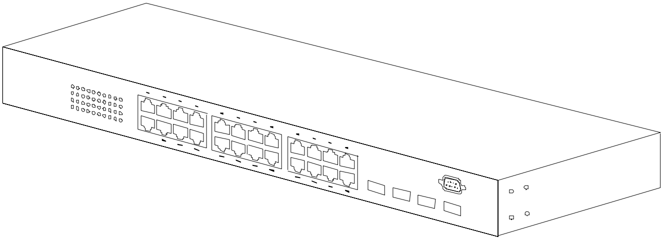
1. **8 * TX + 2 * SFP (10G) ports model**
   This model supports eight TX ports and two extra SFP ports for Gigabit Ethernet connections.



2. **16 * TX + 4 * SFP (16G) ports model**
   This model supports sixteen TX ports and four share SFP ports. Port 13~16 are 1000TX RJ45 port / SFP port optional for Gigabit connection.



3. **24 * TX + 4 * SFP (24G) ports model**
   This model supports twenty-four TX ports and four share SFP ports. Port 21~24 are 1000TX RJ45 port / SFP port optional for Gigabit connection. And they can auto-detect the connection from 1000TX RJ45 port or SFP port.



Contents

1. Introduction

There are three models for the Gigabit Web Smart Switch Series – 8TX+2SFP(10G) model, 16TX+4SFP(16G) model and 24TX+4SFP(24G) model. This Gigabit Web Smart Switch is a Layer2 Web Smart switch with lots of advanced network functions including VLAN, trunking, spanning tree, mirror port, rate limit and port configuration. Console is supported for some basic settings. Web interface is for switch management. IEEE 802.1x is supported for port security application. These functions can meet most of the management request for current network.

1.1 Package Contents

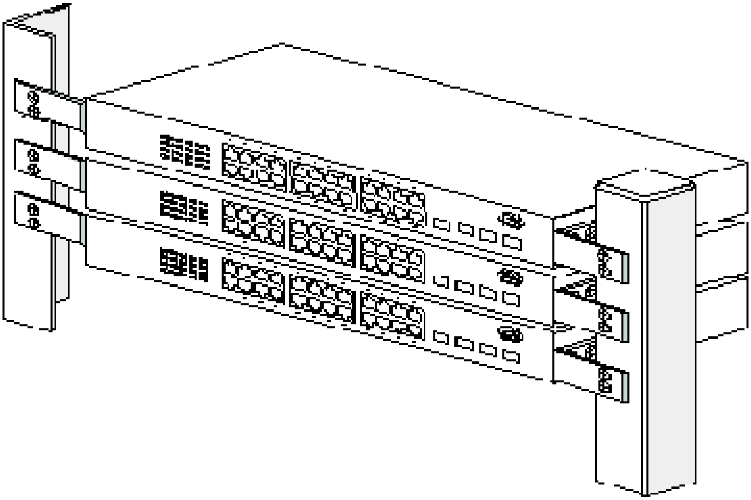
- One Gigabit Web Smart Switch
- One AC power cord
- One console cable
- Two rack-mount kits and screws (*for 16TX+4SFP/24TX+4SFP models only)
- This user's manual

2. Where To Place the Switch

This Switch can be placed on a flat surface (your desk, shelf or table).
Place the Switch at a location with these connection considerations in mind:

- The switch configuration does not break the rules as specified in Section 3.
- The switch is accessible and cables can be connected easily to it.
- The cables connected to the switch are away from sources of electrical interference such as radio, computer monitor, and light fixtures.
- There is sufficient space surrounding the switch to allow for proper ventilation (the switch may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

For 16TX+2SFP/24TX+4SFP model, you can also install the switch on a 19" rack with the rack-mount kits as the picture.



<< Rack-Mount Installation >>

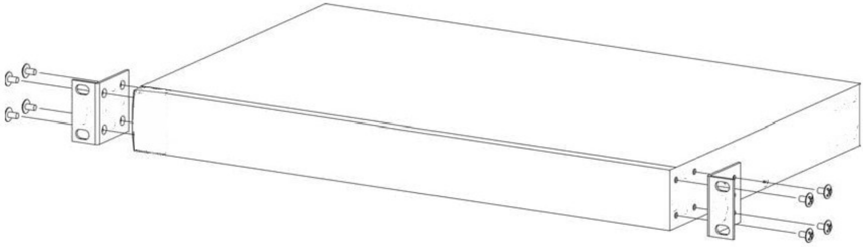
Before rack mounting the switch,please pay attention to the following factors :

1. **Temperature** - Because the temperature in a rack assembly could be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range. (Please refer to Product Specifications in the manual.) Air flow is necessary in a rack for temperature stable.
2. **Mechanical Loading** - Do not place any equipment on top of this rack-mounted switch.
3. **Circuit Overloading** - Be sure that the supply circuit to the rack assembly is

not overload after installing this switch.

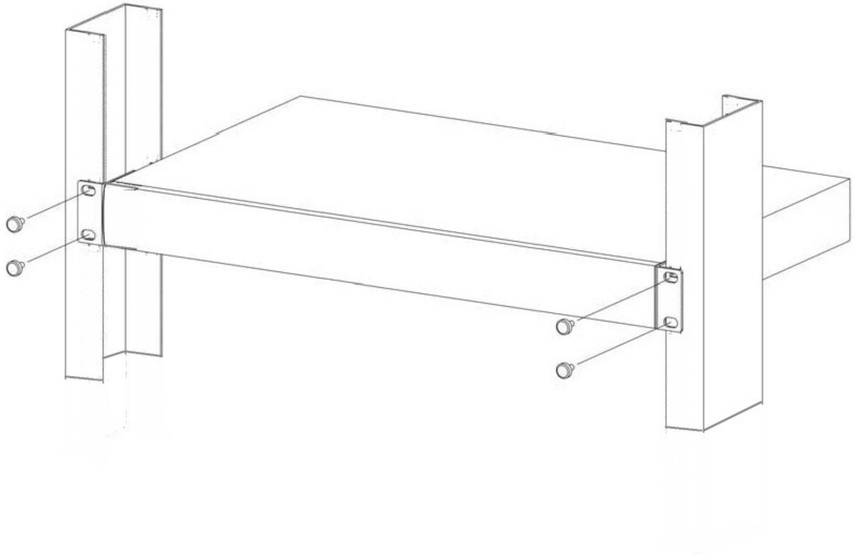
4. **Grounding** - Rack-mounted equipment should be properly and well grounded. Particular attention should be given to supply connections other than direct connections to the mains.

[Attach Rack-Mount Brackets to the Switch]



1. Position a Rack-Mount Bracket on one side of the Switch.
2. Line up the screw holes on the bracket with the screw holes on the side of the switch.
3. Use a screwdriver to install the M3 flat head screws through the mounting bracket holes into the switch. (There could have two or four screws for one bracket. That depends on the model that installed.)
4. Repeat Step 1~3 to install another bracket to the switch.
5. Now it is ready to mount to a rack.

[Mount the Switch on a Rack]



1. Position a bracket that is already attached to the switch on one side of the rack.
2. Line up the screw holes on the bracket with the screw holes on the side of the rack.

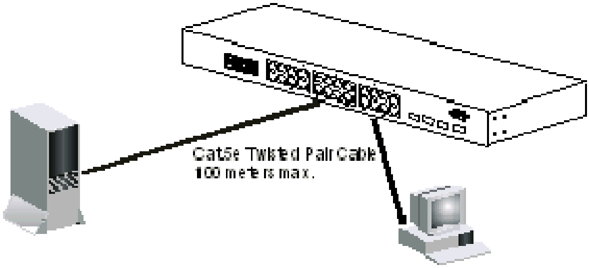
3. Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.
4. Repeat Step 1~3 to attach another bracket that is already attached to the switch on another side of the rack.

3. Configure Network Connection

3.1 Connecting Devices to the Switch

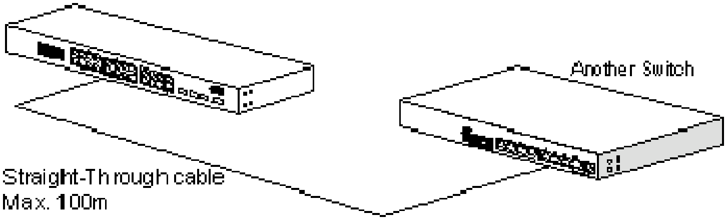
[Connection Guidelines:]

- For 10BaseT connection : Category 3 or 5 twisted-pair Ethernet cable
- For 100BaseTX connection : Category 5 twisted-pair Ethernet cable
- For 1000BaseTX connection: Category 5e or 6 twisted-pair Ethernet cable
- For TX cable connection, always limit the cable distance to 100 meters (328 ft) as defined by IEEE specification
- If your switch has 1000BaseSX/1000BaseLX connections, you can connect long distance fiber optic cable to the switch.
- Because this switch supports **Auto MDI/MDI-X** detection on each TX port, you can use normal straight through cable for both workstation connection and hub/switch cascading.



3.2 Connecting to Another Ethernet Switch/Hub

This Switch can be connected to existing 10Mbps / 100Mbps / 1000Mbps hubs/switches. Because all TX ports on the Switch support Auto MDI/MDI-X function, you can connect from any TX port of the Switch to the MDI or MDI-X port of another hub/switch with Straight Through or Crossover cables. If the switches have fiber-optic ports, you can cascade them with fiber optic cable.

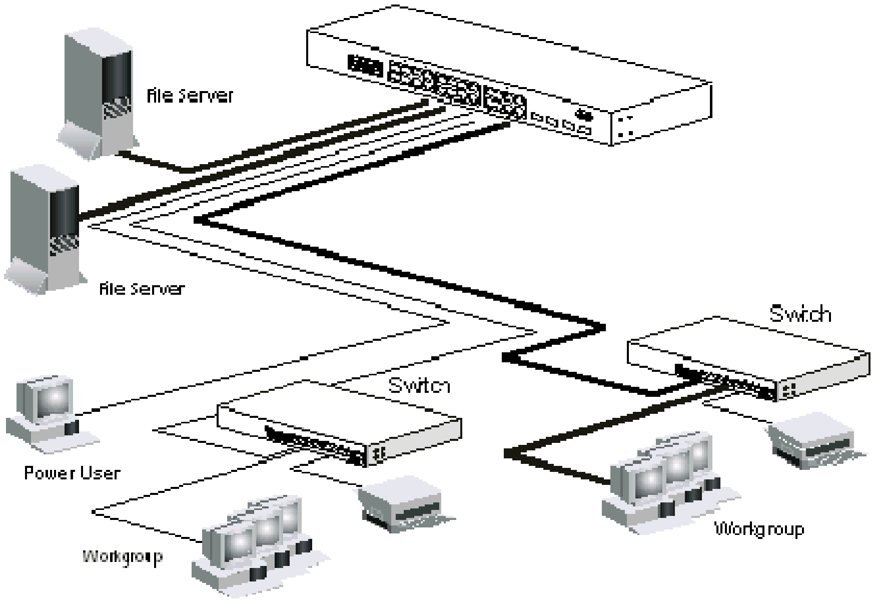


3.3 Application

A switch can be used to overcome the hub-to-hub connectivity limitations as well as improve overall network performance. Switches make intelligent decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary traffic.

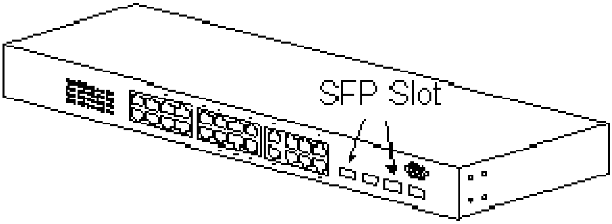
The example below demonstrates the switch ability to segment the network. The number of nodes on each segment is reduced thereby minimizing network contention (collisions) and boosting the available bandwidth per port.

With Web Smart function of the switch, network administrator is easy to monitor network status and configure for different applications.



4. Adding Module

This switch supports SFP (for 1000SX/LX/…) connectors for gigabit ports. Because the SFP slots support hot-swap function, you can plug/unplug the SFP transceiver to/from the SFP slot directly. The switch can auto-detect the gigabit connection from SFP slot.



Follow the steps for module adding and removing.

[Add SFP Transceiver]

1. Plug in the SFP Transceiver to SFP slot directly.
2. Connect network cable to the SFP Transceiver. If the connected devices are working, the Link/Act LED will be ON.

[Remove SFP Transceiver]

Unplug the SFP Transceiver from SFP slot directly.

5. LEDs Conditions Definition

The LEDs provide useful information about the switch and the status of all individual ports.

[For 8TX+2SFP / 16TX+4SFP / 24TX+4SFP Models]

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
System	OFF	System is booting.
	Yellow	System is initializing.
	Green	System is running.
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.
	Green	The connection speed is 1000Mbps.
	Yellow	The connection speed is 10/100Mbps.
FDX/Col.	ON	The connection is Full Duplex.
	Flashing	Collisions happen for Half Duplex.

6. Manage / Configure the switch

6.1 Introduction of the management functions

This switch is a L2 Web Smart switch. It supports in-band management function from Http interface. Console is supported for some basic settings. It supports network configuration functions, like VLAN, Trunking, Port Mirror, QoS, spanning tree and software backup/update. Users can configuration these functions for different network applications. The following is a brief introduction about these functions before the detail operation sections.

1. VLAN (Virtual LAN)

   VLAN can divide the switch to several broadcast domains to prevent network traffic between different user groups. This switch supports 802.1Q tag-based VLAN and Port-based VLAN. Users with the same VLAN ID can transfer data to each other. The network traffic will be blocked if they have different VLAN ID.

2. Trunk

   If two switches are cascaded together, the bottleneck will happen at the cascading connection. If more cables could be used for the cascading connection, it will reduce the bottleneck problem. In normal case, switches will become unstable because of traffic looping when more than one cable is connected between them. If the switches support trunk function, they can treat these cables as one connection between them. The traffic looping will not happen between these cables and the switches will work stable with bigger bandwidth between them.

   Notes: About redundant application

   The trunk connection supports redundant function. If any trunk cable is broken, the traffic going through that cable will be transferred to another trunk cable automatically. For example, if traffic of user port Port 6 is assigned to Port 1 in a Trunk and Port 1 connection breaks, Port 2 will take over the traffic for Port 6 automatically. (It could be used for redundant application.)

3. Spanning Tree Protocol / Rapid Spanning Tree Protocol

   Spanning tree is a protocol to prevent network loop in network topology. If network loop happens, it will cause switches in the network unstable because more and more traffic will loop in the network. If network loop happens, spanning tree protocol will block one connection in the loop automatically. But it will also cause a period of delay (30 seconds for STP and shorter time for RSTP) if any network connection is changed because of the network topology detection operation of the protocol.

   Because there could be more than one switch in the network, users can configure this function for their network spanning tree application.

4. Port Mirror

   This switch operates in store-and-forward algorithm so it is not possible to monitor network traffic from another connection port. But the port mirror function can copy packets from some monitored port to another port for network monitor.

5. QoS
   For Quality of Service request in a network, packets could be classified to different forwarding priorities. For real-time network traffic (like video, audio), it needs higher priority than normal network traffic. With the definition of packet priority, it could have 8 priority levels (from 0 to 7). This switch supports four priority level queues on each port. It could be configured for port-based, 802.1P tagged based, or DiffServ of IP packets priority. User can define the mapping of priority values to the priority queues.

6. Static Mac ID in ARL table
   The switch can learn the Mac address from user's packets and keep these Mac address in the ARL table for store-and-forward table lookup operation. But these Mac addresses will be deleted from ARL table after some time when users do not send any packets to the switch. This operation is called aging and the time is called aging time. It is about 5 minutes normally (it could be changed by users.) If users want to keep a Mac address always in ARL table on some port, they can assign the Mac address to ARL table. These Mac ID are called Static Mac address. This switch supports static Mac address assignment. *The static Mac address assignment will also limit the Mac address could be used on the assigned port only with the port security configuration function.* For example, assigning "00-00-e2-11-22-33" to Port 5 will always keep this Mac ID alive on Port 5 but also limit this Mac address could work on Port 5 only.

   <u>Note</u>: About Static Mac Address Filter-in (port binding) function
   There is a "Mac Security Configuration" function for port security. If it is set to "Accept function", only these static Mac addresses can access network through the assigned port. The other Mac addresses will be forbidden for network access through that port. This function can be used for port binding security application. Please refer to Section 6.3 for the details of the Mac address filter-in operation of the switch.

7. Dynamic Mac ID Number Limit
   Beside Static Mac ID Limit, there is another Dynamic Mac ID Number Limit function for Mac address security on port. This function can limit the Mac ID number to access network through a port. For example, five Mac ID are allowed for Port 2. That means up to five users are allowed, but don't care who the users are. It is done by "Limit by Mac no." option in "Mac Security Configuration" function.

8. IEEE 802.1x Port Security Function
   If the 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It will need a RADIUS server for the authentication function. Users will be asked for username and password before network access. If the RADIUS server authenticates it, the switch will

enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch.

9. Rate Control
   This function can limit the traffic rate for physical ports. The traffic could be ingress traffic or egress traffic. This function can limit the network bandwidth utilization of users.

10. Private VLAN
    Three kinds of VLAN are defined for this application – Primary VLAN, Community VLAN, and Isolated VLAN. Community VLAN and Isolated VLAN can communicate with Primary VLAN, but they cannot communicate with each other. And users in Isolated VLAN cannot communicate with each other. This is a special VLAN configuration. This switch supports a dedicated configure interface for such application.

11. Software Backup/Update
    This switch supports backup and update functions for its internal software and its network configuration. It could be done in two ways.

    a. From console when booting : doing by Xmodem protocol and by terminal program for boot code and run-time code updating..

    b. From web browser : doing by http protocol and by web browser for run-time code and configuration backup/update.

6.2 Basic Settings with Console Connection

Please follow the steps to complete the console hardware connection first.

1. Connect from the console port of the switch to COM port of PC with the console cable.
2. Start the terminal program of Windows. Create a new connection and select COM port of PC used for the console. Set the configuration of the terminal as **[9600,8,N,1]**. (You can find the terminal program in [Start] -> [Programs] -> [Accessory Programs] -> [Communication] -> [Terminal]. If you cannot find it, please install it from your Windows Installation Disk. Please refer to your Windows user manual for the installation.)
3. Power on the switch.

If everything is correct, the booting screen will appear in the terminal program when the switch is powered on. It will stop at the following screen after some initializing messages.

```
----------------------------------------------------------------------------------------------------
......

Start to run system initialization task.
[System Configuration]
Company Name        :
Model Name          : Gigabit Web Smart Switch
MAC    Address      : 00:00:00:01:53:47


Firmware version: 1.01.04 (built at Jul 15 2008 09:19:16)
Press <ENTER> key to start.
----------------------------------------------------------------------------------------------------
```

Press Enter key, user name and password will be requested. The default user name and password is "**admin**" / ”**admin**”.
After login the switch, a prompt will be shown. Because this switch supports command-line for console interface, you can press “**?**” or “**help**” to check the command list first.

With “**?**” command, you can find the command list as follow.

```
----------------------------------------------------------------------------------------------------
>?
[Command List]
?.............. Help commands
default........ Restore to factory default setting
help........... Help commands
logout......... Logout
ping........... Ping a specified host with IP address
reset.......... Reset system
set............ Set commands
show........... Show commands
----------------------------------------------------------------------------------------------------
```

Here is the detail about these commands.

1. **Default** command
   This command is used to restore factory default settings.

   Enter “default” at the prompt, you will be ask to confirm with Yes/No.

   ```
   >default
   All current setting will be lost after restoring default!
   Are you sure to restore default setting now?(Y/N)
   ```

   If “y” is entered, the switch configuration will be set to factory default and reboot. If “n” is entered, just leave and no any action will go.

2. **Help** command
   This is a help command (the same as “?” command) and the switch will prompt with command list.

3. **Logout** command
   This is a logout command.

4. **Ping** command
   User can use this command to ping another network device to verify the network connection and activity. (It is similar to the ping command in MS-DOS.)

   Enter “ping” at the prompt, the command syntax will be shown.

   ```
   >ping
   Syntax: ping [-n count] [-l length] [-t] [-w timeout] ip
   -n count   : Number of echo requests to send.
   -l length : Send buffer size, and length is between 64~8148
   -t         : Ping the specified host until stopped by <ESC> key.
   -w          : Timeout in milliseconds to wait for each reply.
   ip         : IP address (xxx.xxx.xxx.xxx)
   ```

   For example, “ping 192.168.1.80”. “Ctrl-C” can be used to break continuous ping operation.

5. **Reset** command

This command is used to reset switch.

Enter “reset” at the prompt, you will be asked to confirm the action.

```
>reset
Are you sure to reset switch now?(Y/N)
```

If “y” is entered, the switch will reboot. If “n” is entered, just leave and no any action will go.

6. **Set** command

This command can be used to configure IP configuration of the switch and change the username/password of administrator.

Enter “set” at the prompt, the sub-command list will be shown.

```
>set
[Command List]
admin.......... Set administrator name and password
net............ Set network configuration
```

6.1 **set admin** command

This command can be used to modify the user name and password for administrator.

6.2 **set net** command

This command is used to configure IP address of the switch.

Its syntax is . . .

```
>set net
[Syntax]set net [arg_1 data_1] [arg_2 data_2] ... [arg_n data_n]
[Argument List]
dhcp........... Set DHCP client
ip............. Set IP Address
netmask........ Set netmask
gateway........ Set gateway IP address
```

This switch supports DHCP client function. If you set DHCP enable, it will try to get IP configuration from DHCP server when it boots up. You can use “show net” command to check the DHCP setting and current IP configuration of the switch.

If DHCP is enable and the switch cannot find a DHCP server in the network, a message “*BOOTP/DHCP failed on eth0*” will be shown and it will use “192.168.1.1 / 255.255.255.0” as its IP configuration.

If DHCP is enable, you can use the “renew” sub-command to refresh the lease time of the IP address or get the IP configuration again if IP is not got when boot-up.

If you set DHCP disable, you can set the IP configuration with *ip*, *netmask* and *gateway* commands. For example, “set net ip 192.168.1.250 netmask

255.255.255.0 gateway 192.168.1.154" will set these parameters as the IP address configuration of the switch. After the command, you can use "show net" to verify the setting.

7. **Show** command

This command is used to show IP configurations of the switch.

```
>show
[Command List]
net............ Show network configuration
```

7.1 **show net** command will show current IP address configuration of the switch. For example,

```
>show net
[eth0] Network Configuration:
DHCP          : DISABLE
IP Address: 192.168.1.12
Netmask     : 255.255.255.0
Gateway     : 192.168.1.2
```

Note: the default IP configuration of the switch is ...

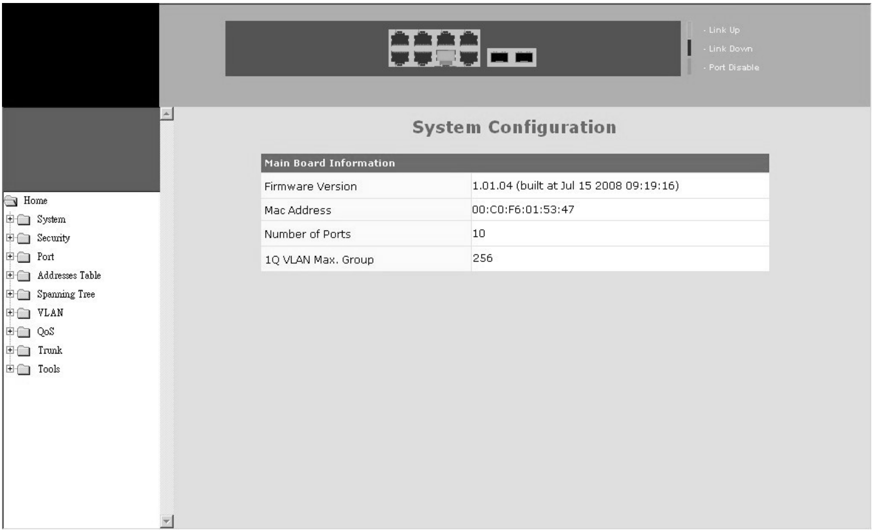
```
DHCP          : DISABLE
IP Address: 192.168.1.1
Netmask     : 255.255.255.0
Gateway     : 192.168.1.254
```

6.3 Management with Http Connection

Users can manage the switch with Http Web Browser connection. Before http connection, IP address configuration of the switch should be done first.

Please follow the instruction in Section 6.2 to complete the console connection and use “**show net**” command to check IP address of the switch first. If users want to change the IP address of the switch, use “**set net ip xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx gateway xxx.xxx.xxx.xxx**” command to modify the IP address of the switch. The default IP configuration is **192.168.1.1**, mask **255.255.255.0** and gateway **192.168.1.254**.

After IP address configuration done and the switch is connected to network, users can start Http connection by entering IP address of the switch to the web address line in Web Browser. A login screen will be prompted for user name and password. The default user name and password is "**admin**" / ”**admin**”. Then the management homepage will appear.



System Configuration

Main Board Information	
Firmware Version	1.01.04 (built at Jul 15 2008 09:19:16)
Mac Address	00:C0:F6:01:53:47
Number of Ports	10
1Q VLAN Max. Group	256

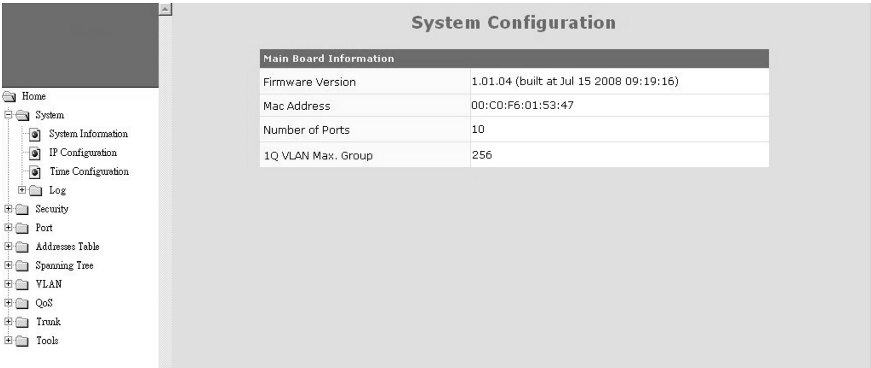
Left part of the homepage is a function list. Users can select one of them for status monitoring or switch configuration.
Upper part of the homepage is the link status of the switch. Three different colors are used to show different status of ports – Link Up, Link Down and Port Disable.
Middle part of homepage is the main operation area for each function.

The details about management with http connection will be shown in the following sub-sections.

6.3.1 System

“System Information” is the homepage of the switch. And there are four sub-functions for it.

1). System Information

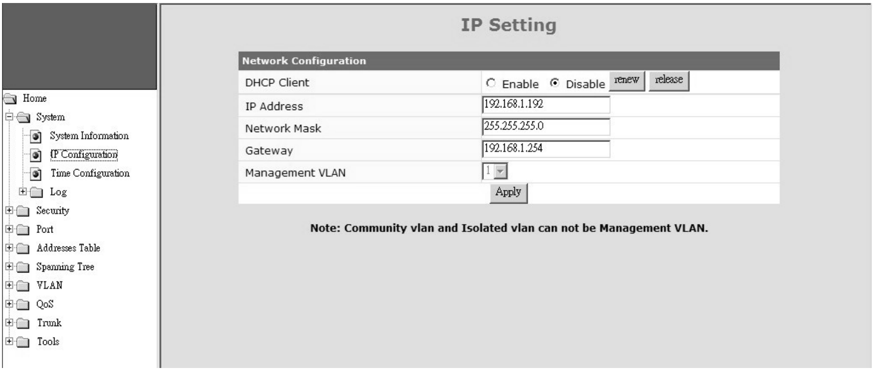


System Configuration

Main Board Information	
Firmware Version	1.01.04 (built at Jul 15 2008 09:19:16)
Mac Address	00:C0:F6:01:53:47
Number of Ports	10
1Q VLAN Max. Group	256

This function lists the system information about the switch. You can find the firmware version, Mac address, connection port number, and maximum VLAN group number here.

2). IP Configuration



IP Setting

Network Configuration	
DHCP Client	○ Enable ● Disable
IP Address	192.168.1.192
Network Mask	255.255.255.0
Gateway	192.168.1.254
Management VLAN	1

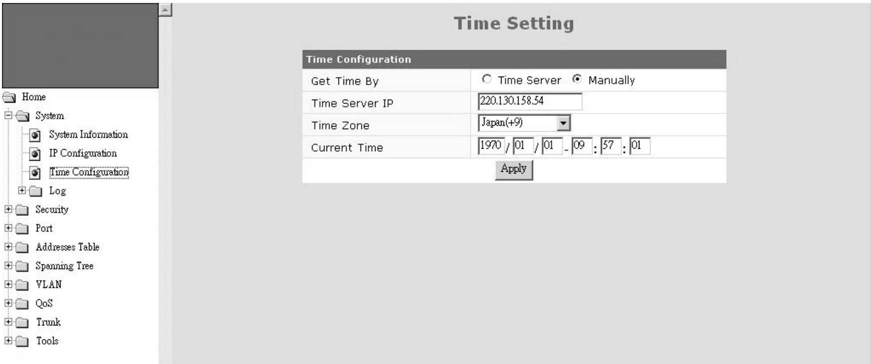
Note: Community vlan and Isolated vlan can not be Management VLAN.

This function is used to setup the IP configuration of the switch.
You can enable DHCP client function to get IP configuration from DHCP server automatically. Or, disable DHCP client function and set IP configuration manually.

Management VLAN : This is used to setup the VLAN ID for remote management interface of the switch. Only users in the same VLAN can manage the switch remotely. For example, setting it to “5” will allow the users in the VLAN with VLAN ID 5 to manage the switch remotely. It works only 802.1Q VLAN function is enable. And please don’t use Community VLAN and Isolated VLAN of Private VLAN as management VLAN. It is caused by the limitation of Private VLAN function.

About DHCP Client [renew] and [release] button ...
[renew] button: If DHCP client function is enabled, you can click [renew] button to refresh the lease time of the IP address. If IP configuration is not got when boot-up, clicking [renew] button will try to get IP configuration again.
[release] button: If DHCP client function is enabled and IP configuration is got, clicking [release] button will release current IP configuration. After that, you can click [renew] button to get the IP configuration again.

3). Time Configuration



Time Setting

Time Configuration	
Get Time By	○ Time Server ● Manually
Time Server IP	220.130.158.54
Time Zone	Japan(+9)
Current Time	1970 / 01 / 01 _ 09 : 57 : 01

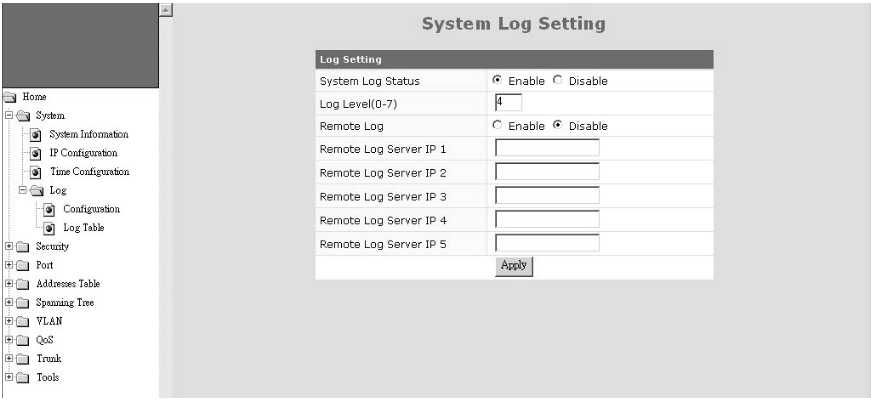
There are two ways to get the system time.

a). Get time from Time Server
This switch support NTP protocol to get time from Internet time server. For such application, you have to select “Get Time by Time Server”, input the IP of Time Server, and select the Time Zone of your location. Then click [Apply]
If time is got from Time Server, it will be shown at “Current Time”.
For such application, you have to get the IP of Time Server from your network administrator first.

b). Set time manually
This switch can count time internal. You can select “Get Time by Manually”, and input current time manually. Then click [Apply].

4). Log

[Configuration]



System Log Setting

Log Setting	
System Log Status	● Enable ○ Disable
Log Level(0-7)	4
Remote Log	○ Enable ● Disable
Remote Log Server IP 1	
Remote Log Server IP 2	
Remote Log Server IP 3	
Remote Log Server IP 4	
Remote Log Server IP 5	
	Apply

Users can configure System Log function and view log records here. If this function is enabled, the switch will record events to a log file and put the log file to flash.

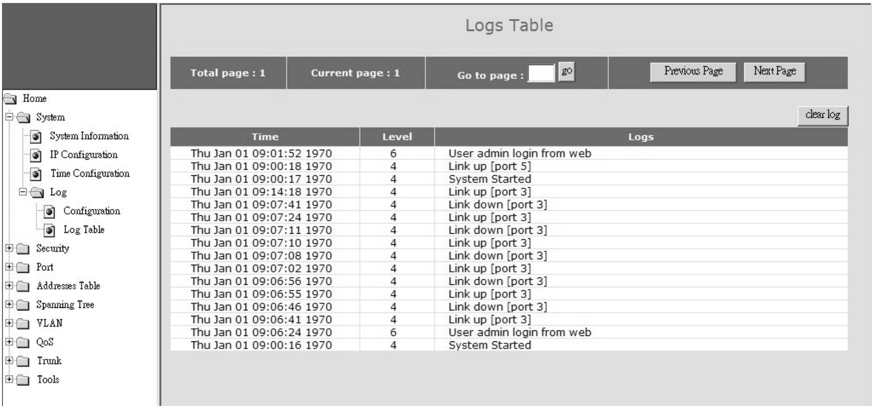
Up to 512 records are allowed for local logging. If more than 512 events happen, the records will be overwritten from beginning. And if remote syslog server is applied, the switch will also send event record to the syslog server.

About log function configuration ...
System Log Status : This can enable/disable system logging function.
Log Level (0~7) : Log levels 0~7 are defined ad below.

Level	Name	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	Informational messages
7	Debug	Debug-level messages

Remote Log : This can enable/disable remote syslog function.
Remote Log Server IP : This is the syslog server IP for remote logging. Up to five syslog servers is supported. Event logs will be sent to those syslog servers at the same time.

[Log Table]



Logs Table

Total page : 1 | Current page : 1 | Go to page :

Time	Level	Logs
Thu Jan 01 09:01:52 1970	6	User admin login from web
Thu Jan 01 09:00:18 1970	4	Link up [port 5]
Thu Jan 01 09:00:17 1970	4	System Started
Thu Jan 01 09:14:18 1970	4	Link up [port 3]
Thu Jan 01 09:07:41 1970	4	Link down [port 3]
Thu Jan 01 09:07:24 1970	4	Link up [port 3]
Thu Jan 01 09:07:11 1970	4	Link down [port 3]
Thu Jan 01 09:07:10 1970	4	Link up [port 3]
Thu Jan 01 09:07:08 1970	4	Link down [port 3]
Thu Jan 01 09:07:02 1970	4	Link up [port 3]
Thu Jan 01 09:06:56 1970	4	Link down [port 3]
Thu Jan 01 09:06:55 1970	4	Link up [port 3]
Thu Jan 01 09:06:46 1970	4	Link down [port 3]
Thu Jan 01 09:06:41 1970	4	Link up [port 3]
Thu Jan 01 09:06:24 1970	6	User admin login from web
Thu Jan 01 09:00:16 1970	4	System Started

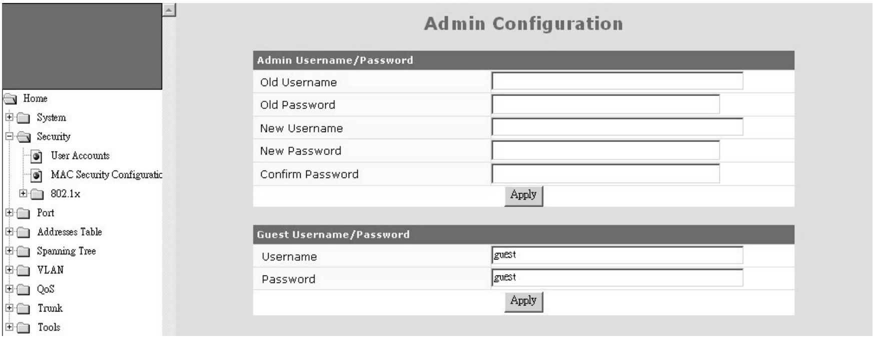
You can view log content here. There could be more than one page. You may change the page or go to a page by its operation icons.

Clicking [clear log] button will clear the local log table.

6.3.2 Security

This function is used to configure security functions of the switch. Those security functions are Administrator Management Security, Mac ID Access Security, and 802.1x Authentication Security.

1). User Accounts (Administrator Management Security)



Admin Configuration

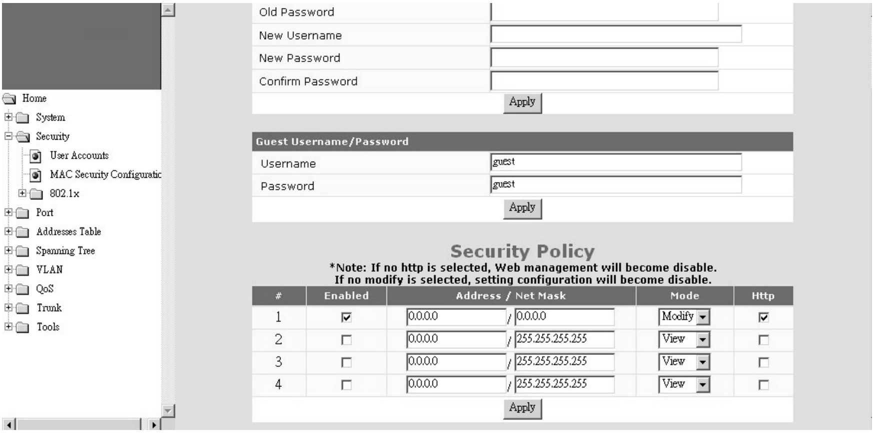
Admin Username/Password	
Old Username	
Old Password	
New Username	
New Password	
Confirm Password	

Guest Username/Password	
Username	guest
Password	guest

Administrator Username/Password : This is for network administrator to change his/her username and password. (Default is admin/admin.)

Guest Username/Password : This is used to setup the username/password of guest-right user who just can view the setting of the switch.

[Security Policy]



Old Password	
New Username	
New Password	
Confirm Password	

Guest Username/Password	
Username	guest
Password	guest

Security Policy

*Note: If no http is selected, Web management will become disable.
If no modify is selected, setting configuration will become disable.

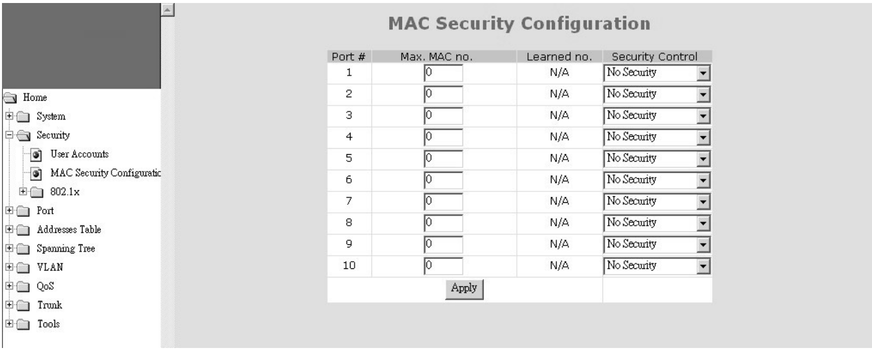
#	Enabled	Address / Net Mask		Mode	Http
1	☑	0.0.0.0	/ 0.0.0.0	Modify	☑
2	□	0.0.0.0	/ 255.255.255.255	View	□
3	□	0.0.0.0	/ 255.255.255.255	View	□
4	□	0.0.0.0	/ 255.255.255.255	View	□

This is used to setup the IP addresses that can manage this switch. They have different access rights set in "Mode". And the remote management interfaces

(Http) could be enable/disable for different administrators. This is for security policy for switch management.

Note: Remember to enable at least one IP/Subnet with Modify right for Http interface. Otherwise, configuring switch from remote will become impossible. In that case, you have to use the “default” command from console to restore settings to factory default for switch management.

2). Mac Security Configuration



MAC Security Configuration

Port #	Max. MAC no.	Learned no.	Security Control
1	0	N/A	No Security
2	0	N/A	No Security
3	0	N/A	No Security
4	0	N/A	No Security
5	0	N/A	No Security
6	0	N/A	No Security
7	0	N/A	No Security
8	0	N/A	No Security
9	0	N/A	No Security
10	0	N/A	No Security

There two Mac ID security modes for the switch. One is Static Mac ID Filter on Port, another is Dynamic Mac ID Number Limit on Port.

[Static Mac ID Filetr on Port]
This function can limit only those static Mac addresses on the port can access network. Other Mac addresses will be rejected by the port. Sometimes it is called “Mac-Port Binding”.

Follow the steps to configure it.

a. Set the “Security Control” to “Accept” on those ports that will apply static Mac ID security. Then click [Apply].
b. Set Static Mac Addresses that are allowed for network access at [Static Address] of [Address Table] function. Please refer to that section for the details.

[Dynamic Mac ID Number Limit on Port]
This function can limit the Mac ID number to access network through a port. For example, five Mac ID are allowed for Port 2. That means up to five users are allowed, but don’t care who the users are.

Follow the steps to configure it.

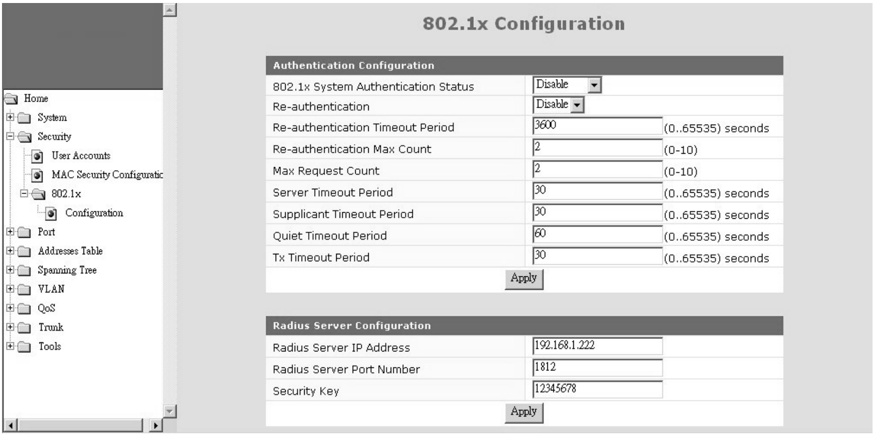
a. Set the “Security Control” to “Limited by MAC no.” on those ports that will apply dynamic Mac ID number security. And set the “Max. MAC no.” to the users number allowed on the ports.

b. Then click [Apply].

The switch will learn users automatically and show current user number at “Learned no.”.

3). 802.1x Configuration

If 802.1x function is enabled, the switch will act as an authenticator for users accessing network through the switch. It will need a RADIUS server for the authentication function. Users will be asked for username and password before network access. If the RADIUS server authenticates it, the switch will enable the port for network access. This function is very useful for network security application to prevent illegal users access network through the switch.



802.1x Configuration

Authentication Configuration		
802.1x System Authentication Status	Disable	
Re-authentication	Disable	
Re-authentication Timeout Period	3600	(0..65535) seconds
Re-authentication Max Count	2	(0-10)
Max Request Count	2	(0-10)
Server Timeout Period	30	(0..65535) seconds
Supplicant Timeout Period	30	(0..65535) seconds
Quiet Timeout Period	60	(0..65535) seconds
Tx Timeout Period	30	(0..65535) seconds

Radius Server Configuration	
Radius Server IP Address	192.168.1.222
Radius Server Port Number	1812
Security Key	12345678

The function here is for 802.1x function configuration.

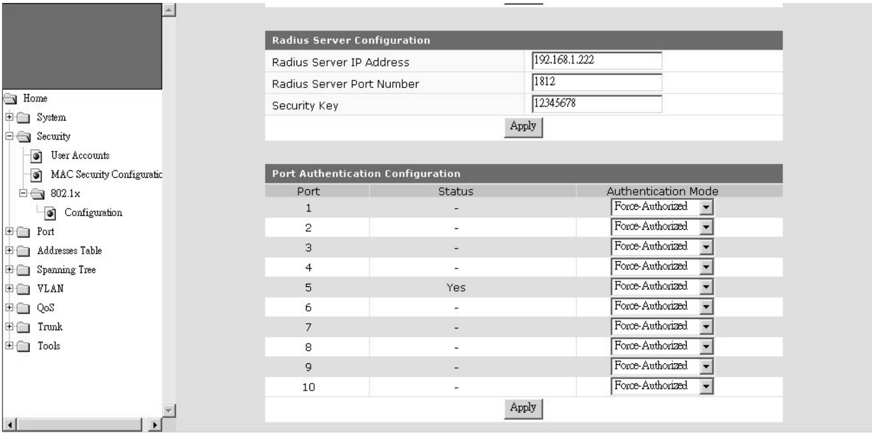
1. **802.1x Authentication Status**: [Enable/Disable/Transparent]
   Enable: enable 802.1x function in authentication mode
   Disable: disable 802.1x function
   Transparent: only forwarding 802.1x packets
2. **Re-authentication (enable/disable)**, **Timeout Period** and **Max Count**:
   The re-authentication function will re-authenticate users after the timeout period. The Max Count is the maximum re-try count between the switch and users before authentication fail.
3. **Max Request Count** and **Server Timeout Period**:
   The Server Timeout Period is the timeout period for the request between the switch and RADIUS server.
   The Max Request Count is the maximum re-try count between the switch and RADIUS server before authentication fail.
4. **Supplicant Timeout Period**:
   This is the timeout value between the switch and users (called “supplicant” in 802.1x) after first identification. The valid value is 0~65535.

5. **Quiet Timeout Period**:
   This is the quiet time value between the switch and the user before next authentication process when authentication fails.
6. **Tx Timeout Period**:
   This is the timeout value for the identification request from the switch to users. The request will be re-tried until the **Re-authentication Max Count** is met. After that, authentication fail message will be sent. The valid value is 0~65535.

[Radius Server Configuration]

This function is for configuration between switch and RADIUS server. You can assign the IP address of Radius Server, the protocol port number, and the security key.

[Port Authentication Configuration]



Radius Server Configuration

Radius Server IP Address	192.168.1.222
Radius Server Port Number	1812
Security Key	12345678

Apply

Port Authentication Configuration

Port	Status	Authentication Mode
1	-	Force-Authorized
2	-	Force-Authorized
3	-	Force-Authorized
4	-	Force-Authorized
5	Yes	Force-Authorized
6	-	Force-Authorized
7	-	Force-Authorized
8	-	Force-Authorized
9	-	Force-Authorized
10	-	Force-Authorized

Apply

The Port Authentication Configuration is used to select the authentication mode for each port of the switch.

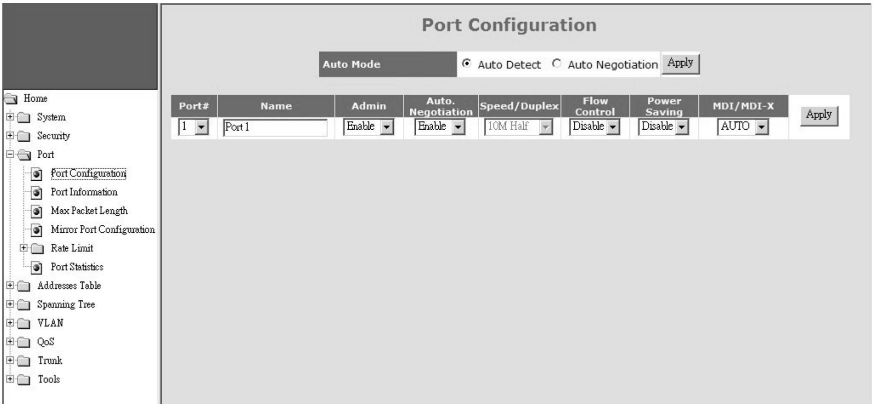
1. Auto: This is the normal 802.1x operation mode. The authentication status (authenticated or unauthenticated) depends on the authentication result of port.
2. Force-Authorized: This mode will force the port always being authentication successful in 802.1x process and the real authentication result will be ignored.
3. Force-Unauthorized: This mode will force the port always being authentication fail in 802.1x process and the real authentication result will be ignored.
4. None: This mode will disable 802.1x operation on this port.

And you can see current 802.1x status on each port.

6.3.3 Port

This section is about configurations for ports. For port speed setting, maximum packet size setting, mirror port setting, port bandwidth limit, and port statistics.

1). Port Configuration



Port Configuration

Auto Mode ● Auto Detect ○ Auto Negotiation Apply

Port#	Name	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	Power Saving	MDI/MDI-X	
1	Port 1	Enable	Enable	10M Half	Disable	Disable	AUTO	Apply

This function is used to configure port settings of the switch. You can enable /disable a port, set it to fixed 10M or 100M or 1000M ... and so on.

Auto Mode : User can select the operation mode of port when "auto" is set to disabled.

For "Auto Negotiation" mode, the switch will do port auto-negotiation function ON/OFF when the auto function of port (in Port Configuration setting) is enabled/disabled.

For "Auto Detect" mode, the switch will always keep port auto-negotiation function ON but just modify its attribution if auto function of port (in Port Configuration setting) is disabled.

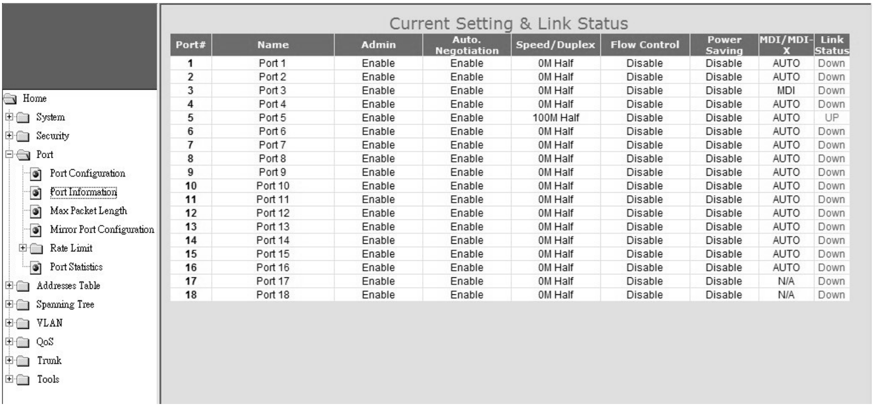
For applications, you should select "Auto Detect"mode if the connected device is auto-negotiation enabled. (For example, customer's PC is auto-negotiation enable and you want to set his network connection to work at 10Mbps.)
And you can select "Auto Negotiation"mode if the connected device is auto-negotiation disabled (it is called forced mode, sometimes). Some of old TX-FX Converters needs to work in this mode because FX supports 100/Full forced mode only.

For most applications, "Auto Detect" mode is OK.

Port Setting : It is for modifying the setting of port. Follow the steps to do it.

1. Select the port that you want to modify in “Port#” first.
2. Fill the name of the port.
3. Select Enable/Disable state in “Admin”. If Disable is selected, this port will be disabled for any network access.
4. Select the Enable/Disable state of Auto function of port. The auto mode could be auto-negotiation or auto-detect operation when auto is set to disable.
5. If Auto is disabled, select the operation speed and duplex mode of the port in “Speed/Duplex”.
6. Select the Enable/Disable state of Flow Control function of port.
7. Select the Enable/Disable state of Power Saving function of port. If it is enabled, port will go to low power state when link down.
8. Select the MDI/MDI-X operation mode. It could be “Auto”, “MDI”, or “MDI-X”. “Auto” can auto-detect and get the correct connection mode. “MDI” will set the port to MDI mode for switch-to-switch connection. “MDI-X” will set the port to MDI-X mode for user PC connection.
9. Click [Apply] after any modification.

2). Port Information



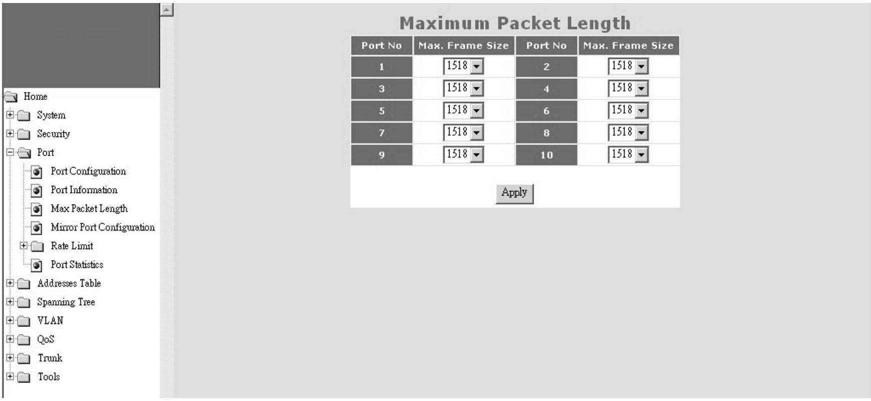
Current Setting & Link Status

Port#	Name	Admin	Auto. Negotiation	Speed/Duplex	Flow Control	Power Saving	MDI/MDI-X	Link Status
1	Port 1	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
2	Port 2	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
3	Port 3	Enable	Enable	0M Half	Disable	Disable	MDI	Down
4	Port 4	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
5	Port 5	Enable	Enable	100M Half	Disable	Disable	AUTO	UP
6	Port 6	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
7	Port 7	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
8	Port 8	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
9	Port 9	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
10	Port 10	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
11	Port 11	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
12	Port 12	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
13	Port 13	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
14	Port 14	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
15	Port 15	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
16	Port 16	Enable	Enable	0M Half	Disable	Disable	AUTO	Down
17	Port 17	Enable	Enable	0M Half	Disable	Disable	N/A	Down
18	Port 18	Enable	Enable	0M Half	Disable	Disable	N/A	Down

Current Setting & Link Status : It is current status of ports.

Name: The name of the port.
Admin: It shows current port enable/disable status.
AutoNegatiation: It shows current Auto enable/disable status of ports.
Speed/Duplex: It will show current working speed and duplex mode if ports are link up. Or the setting of speed/duplex when auto is disable.
Flow Control: It shows current Flow Control function status of ports.
Power Saving: It shows current Power Saving enable/disable status of ports.
MDI/MDI-X: It shows current MDI/MDI-X setting of ports.
Link: It shows the link status of each port.

3). Max Packet Length



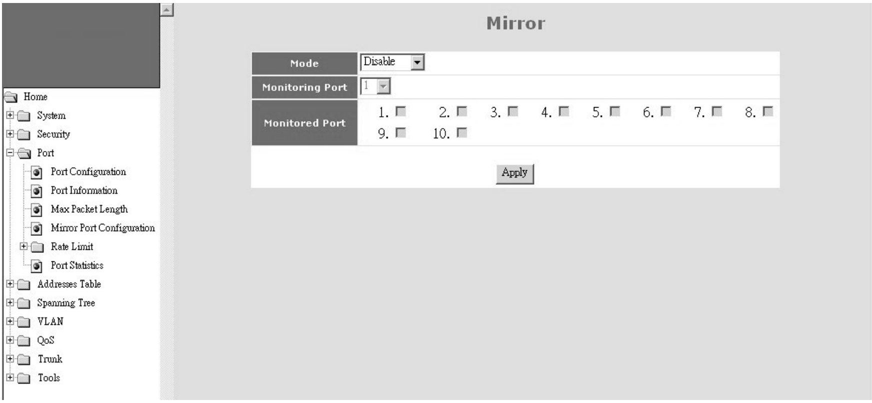
Maximum Packet Length

Port No	Max. Frame Size	Port No	Max. Frame Size
1	1518	2	1518
3	1518	4	1518
5	1518	6	1518
7	1518	8	1518
9	1518	10	1518

This switch supports Jumbo Frame function. And the maximum packet size could be up to 9600 byte/packet. You can select the maximum packet size for each port here.

4). Mirror Port Configuration

This switch operates in store-and-forward algorithm so it is not possible to monitor network traffic from another connection port. But the port mirror function can copy packets from some monitored port to another port for network monitor.



Mirror

Mode	Disable
Monitoring Port	1
Monitored Port	1. □ 2. □ 3. □ 4. □ 5. □ 6. □ 7. □ 8. □ 9. □ 10. □

Mode: This is used to enable/disable Mirror function.
Monitering Port: This is used to set the capture port. The switch will copy the traffic from Monitored Port to this port if Mirror function is enabled.

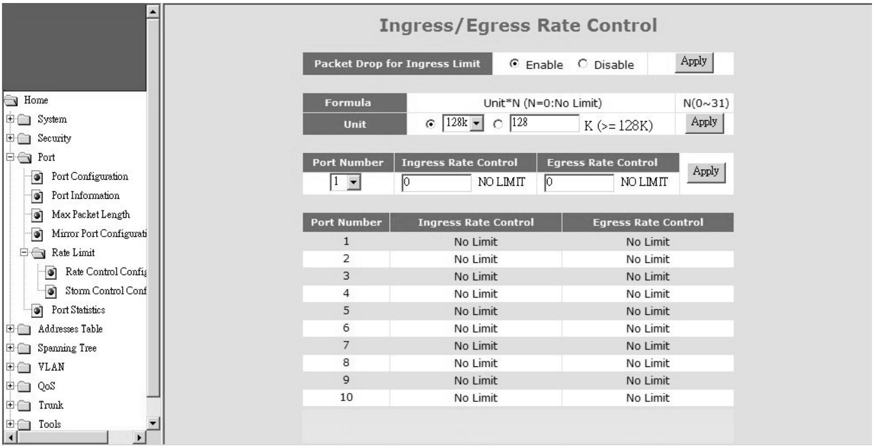
Monitored Port: This is the monitored port. The switch will copy the traffic from this port to Monitoring Port.

5). Rate Control

Two traffic rates could be controlled by the switch. One is the ingress/egress traffic of each port. Another is Broadcast/Multicast/Unicast Storm Control.

5-1) Rate Control Configuration

This function can setup the ingress and egress rate limit of ports.



Ingress/Egress Rate Control

Packet Drop for Ingress Limit	● Enable ○ Disable	Apply

Formula	Unit*N (N=0:No Limit)	N(0~31)
Unit	● 128k ○ 128 K (>= 128K)	Apply

Port Number	Ingress Rate Control	Egress Rate Control	
1	0 NO LIMIT	0 NO LIMIT	Apply

Port Number	Ingress Rate Control	Egress Rate Control
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit

Follow the steps to configure ...

a. Set "Unit" first. It could be selected from pre-defined units, or define by user. Click [Apply] after the setting.

b. Select the Port Number.

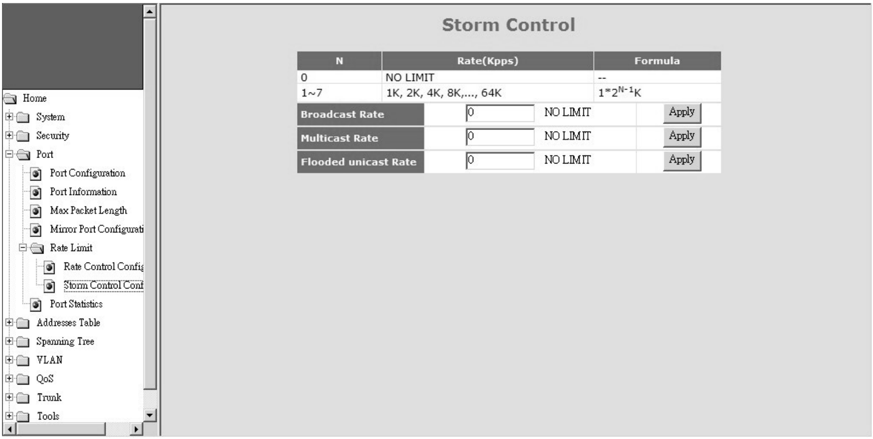
c. Enter the rate limit number for Ingress and Egress traffics. "0" means NO LIMIT. Click [Apply] after the setting.

About "Packet Drop for Ingress Limit" function ...

When Ingress traffic rate exceeds Ingress Rate Limit, the switch can drop packets or pause the traffic. If packet drop is enabled, flow control of ports will be disabled and packets could be dropped. If packet drop is disabled, flow control of ports will be enabled and pause frame will be sent when ingress traffic rate exceeds the limit.

5-2) Storm Control Configuration

This function can setup the broadcast, multicast, and unicast storm rate of the switch.



Storm Control

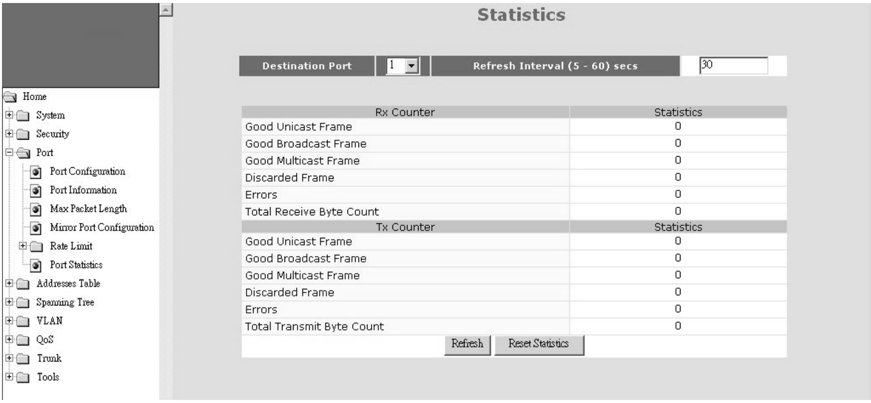
N	Rate(Kpps)	Formula
0	NO LIMIT	--
1~7	1K, 2K, 4K, 8K,..., 64K	$1*2^{N-1}K$

Broadcast Rate	0	NO LIMIT	Apply
Multicast Rate	0	NO LIMIT	Apply
Flooded unicast Rate	0	NO LIMIT	Apply

Please follow the rules in table to setup the maximum storm rates.

Note: The storm rate is counted by pps (packet per second).

6). Port Statistics



Statistics

Destination Port	1	Refresh Interval (5 - 60) secs	30

Rx Counter	Statistics
Good Unicast Frame	0
Good Broadcast Frame	0
Good Multicast Frame	0
Discarded Frame	0
Errors	0
Total Receive Byte Count	0
Tx Counter	Statistics
Good Unicast Frame	0
Good Broadcast Frame	0
Good Multicast Frame	0
Discarded Frame	0
Errors	0
Total Transmit Byte Count	0

Port statistics counters could be read here.
Select a port to get its counters.

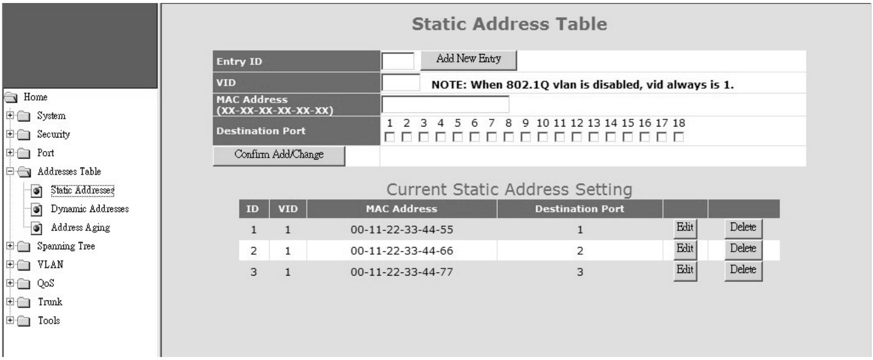
[Refresh]
The counters will be refreshed automatically. You can modify the refresh interval.
And you can click [Refresh] to refresh the counters immediatelly.

[Reset Counters]
Click [Reset Statistics] can reset the counters to “0”.

6.3.4 Address Table

These are functions about Mac address table. One is “Static Address Assign” and another is “Aging Time Setup”.

1). Static Addresses



Static Address Table

Entry ID	[ ] Add New Entry
VID	[ ] NOTE: When 802.1Q vlan is disabled, vid always is 1.
MAC Address (XX-XX-XX-XX-XX-XX)	[ ]
Destination Port	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □
Confirm Add/Change	

Current Static Address Setting

ID	VID	MAC Address	Destination Port		
1	1	00-11-22-33-44-55	1	Edit	Delete
2	1	00-11-22-33-44-66	2	Edit	Delete
3	1	00-11-22-33-44-77	3	Edit	Delete

This switch supports static Mac address assignment. You can assign static Mac addresses by the following steps ...

a. Give an Entry ID. This ID is used as the index of the entry in Static Address Table.
b. Give the VLAN ID. If 802.1Q is disable, the VID will always be 1. This VID will put the static Mac address in some VLAN for 802.1Q VLAN operation.
c. Fill the Mac address. This is the Static Mac Address for this entry.
d. Select the port for this Static Address.
e. Click [Confirm Add/Change] button.

Then this entry will be added to the table.
In “Current Static Address Setting” table, you can edit and delete an entry. (Different Mac Address will be another entry. Mac Address is not allowed to edit for an entry.)

The switch will not age out these static Mac addresses. But there is a limitation for these static Mac addresses - *they are allowed to work on the assigned port only because they are static fixed on the assigned port*.

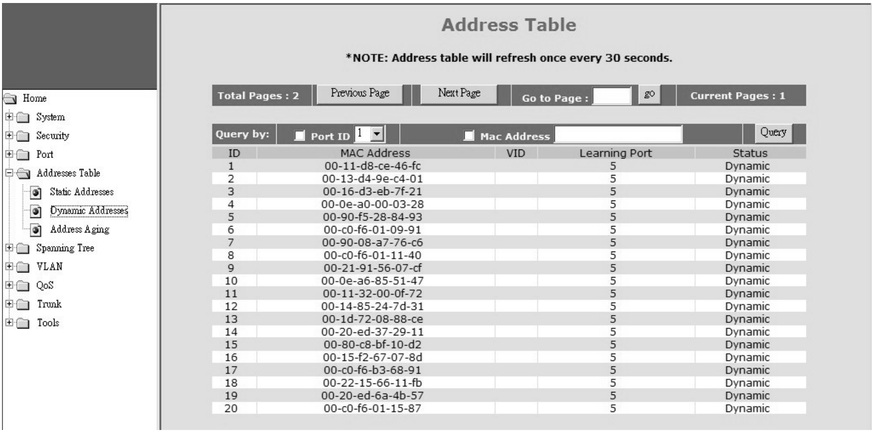
If you want to delete an entry in the static Mac address table, click [Delete] button of the entry and the static Mac address will be removed from the table.

If you want to modify an entry, click [Edit] button of the entry. Do the modification and click [Confirm Add/Change] button. (Different Mac Address will be another entry. Mac Address is not allowed to edit for an entry.)

About Port Security function . . .

You can configure “Mac Security Configuration” function (in “Security” page) for port access security with Mac address. Select “Accept” for such security application..

2). Dynamic Addresses



Address Table

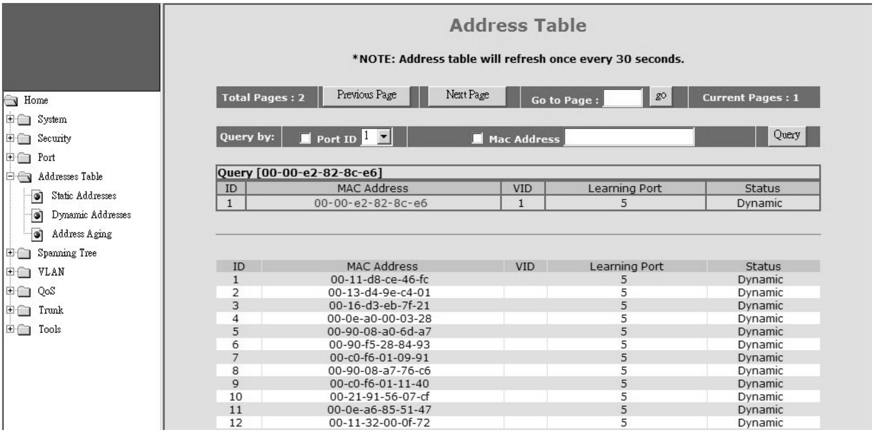
*NOTE: Address table will refresh once every 30 seconds.

ID	MAC Address	VID	Learning Port	Status
1	00-11-d8-ce-46-fc		5	Dynamic
2	00-13-d4-9e-c4-01		5	Dynamic
3	00-16-d3-eb-7f-21		5	Dynamic
4	00-0e-a0-00-03-28		5	Dynamic
5	00-90-f5-28-84-93		5	Dynamic
6	00-c0-f6-01-09-91		5	Dynamic
7	00-90-08-a7-76-c6		5	Dynamic
8	00-c0-f6-01-11-40		5	Dynamic
9	00-21-91-56-07-cf		5	Dynamic
10	00-0e-a6-85-51-47		5	Dynamic
11	00-11-32-00-0f-72		5	Dynamic
12	00-14-85-24-7d-31		5	Dynamic
13	00-1d-72-08-88-ce		5	Dynamic
14	00-20-ed-37-29-11		5	Dynamic
15	00-80-c8-bf-10-d2		5	Dynamic
16	00-15-f2-67-07-8d		5	Dynamic
17	00-c0-f6-b3-68-91		5	Dynamic
18	00-22-15-66-11-fb		5	Dynamic
19	00-20-ed-6a-4b-57		5	Dynamic
20	00-c0-f6-01-15-87		5	Dynamic

This function can show the dynamic Mac addresses learned by the switch. This table will refresh every 30 seconds.

The address table could be more than one page. You can click [Previous Page], [Next Page] to change page. Or, give the page number directly.

Query function is supported by the switch. It could be queried by Port or queried by Mac Address. Select the query function and input the query target. Then click [Query]. The result will be shown.
For example,



Address Table

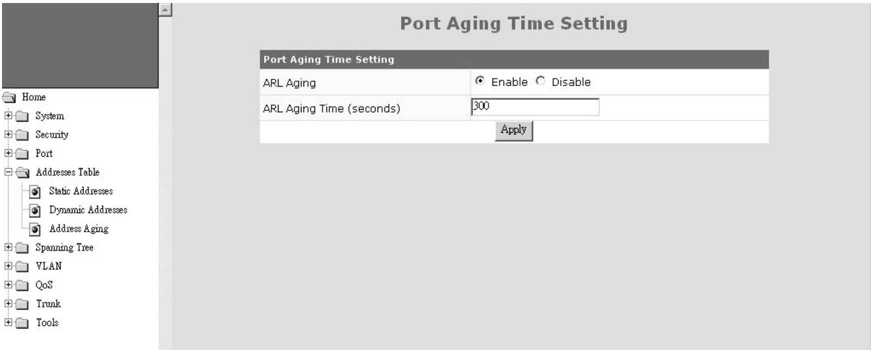
*NOTE: Address table will refresh once every 30 seconds.

Query [00-00-e2-82-8c-e6]

ID	MAC Address	VID	Learning Port	Status
1	00-00-e2-82-8c-e6	1	5	Dynamic

ID	MAC Address	VID	Learning Port	Status
1	00-11-d8-ce-46-fc		5	Dynamic
2	00-13-d4-9e-c4-01		5	Dynamic
3	00-16-d3-eb-7f-21		5	Dynamic
4	00-0e-a0-00-03-28		5	Dynamic
5	00-90-08-a0-6d-a7		5	Dynamic
6	00-90-f5-28-84-93		5	Dynamic
7	00-c0-f6-01-09-91		5	Dynamic
8	00-90-08-a7-76-c6		5	Dynamic
9	00-c0-f6-01-11-40		5	Dynamic
10	00-21-91-56-07-cf		5	Dynamic
11	00-0e-a6-85-51-47		5	Dynamic
12	00-11-32-00-0f-72		5	Dynamic

3). Address Aging



Port Aging Time Setting

Port Aging Time Setting	
ARL Aging	● Enable ○ Disable
ARL Aging Time (seconds)	300

The switch will learn Mac addresses to an ARL table automatically. And follow the table to do packet store-and-forward operation. If Mac addresses are not received for some time, those Mac addresses will be removed from the table. This operation is called aging.

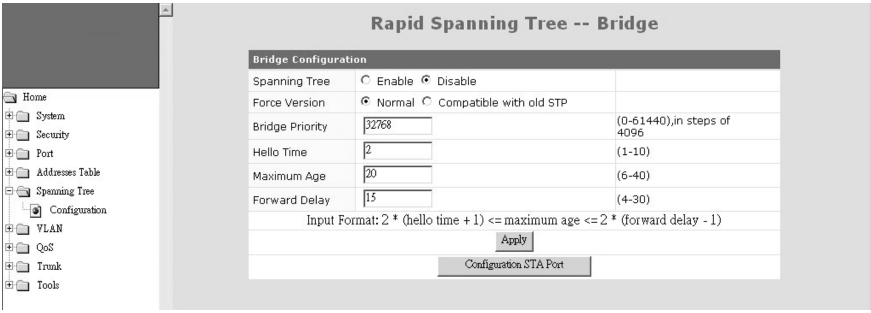
The aging operation could be disable here. And all the learned Mac addresses will not be removed from the ARL table.

And the time for aging operation could be modified here. It is 300 seconds by default.

6.3.5 Spanning Tree

Spanning Protocol can prevent traffic looping in network. It can be configured for switch unit (bridge) and port unit. If spanning tree function is enabled, any link down to link up will have several seconds delay for the port going to forwarding state.

[Setting of Bridge]



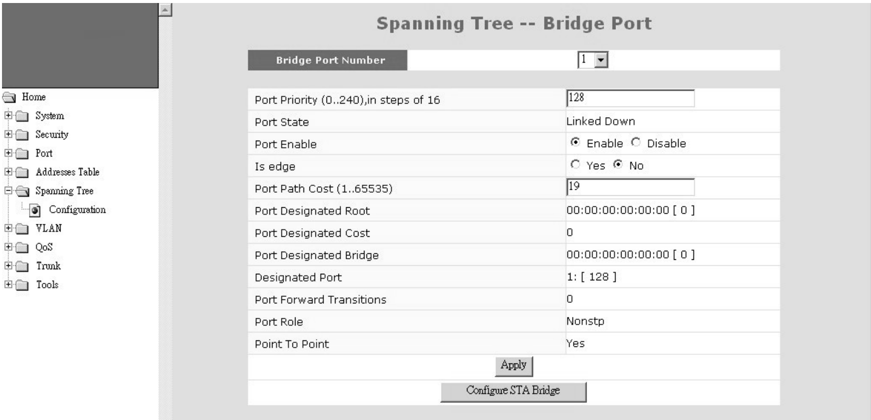
Rapid Spanning Tree -- Bridge

Bridge Configuration		
Spanning Tree	○ Enable ● Disable	
Force Version	● Normal ○ Compatible with old STP	
Bridge Priority	32768	(0-61440),in steps of 4096
Hello Time	2	(1-10)
Maximum Age	20	(6-40)
Forward Delay	15	(4-30)
Input Format: 2 * (hello time + 1) <= maximum age <= 2 * (forward delay - 1)		

Here are the parameters for Spanning Tree operation on the switch.
Enable/Disable : enable/disable spanning tree operation
Force Version : It will operate as Rapid Spanning Tree in “Normal” state. And it can be forced to operate at old Spanning Tree mode if “Compatible with old STP” is selected.
Bridge Priority (0~61440) : Bridge priority is for selecting the root device, root port, and designated port. The device with the highest priority (lowest value) becomes the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time (1~10) : the period to send the spanning tree maintenance packet if the switch is the root of the spanning tree. Default is 2 seconds.
Maximum Age (6~40) : the spanning tree aging time if no spanning tree maintenance packet is received. It will cause the spanning tree to re-create. Default is 20 seconds.
Forward Delay (4~30): the maximum waiting time before changing states (i.e., learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.

The parameters have relation with each other. And here is the rule for it.
2*(Hello Time +1) is less or equal to Maximum Age, and Maximum Age is less or equal to 2*(Forward Delay -1).

[Setting of Port]
Click [Configuration STA Port]. You can configure RSTP/STP on ports.



Spanning Tree -- Bridge Port

Bridge Port Number	1
Port Priority (0..240),in steps of 16	128
Port State	Linked Down
Port Enable	● Enable ○ Disable
Is edge	○ Yes ● No
Port Path Cost (1..65535)	19
Port Designated Root	00:00:00:00:00:00 [0]
Port Designated Cost	0
Port Designated Bridge	00:00:00:00:00:00 [0]
Designated Port	1: [128]
Port Forward Transitions	0
Port Role	Nonstp
Point To Point	Yes

Bridge Port Number is the Ethernet port that will be configured.

Port Priority (0~240) : If the path cost for all ports on a switch are the same, the port with the highest priority (lowest value) will be forwarded when looping happens. If more than one port have the same highest priority, the port with lowest port number will be forwarded.

Port State : It is current spanning tree operation state of the port.

Port Enable : enable/disable spanning tree function on the port.

Is edge : If this switch is at “edge” of the network tree, please select “Yes”. If there are another switches connected, please select “No”. This parameter is used by RSTP to increase its operation speed.

Port Path Cost (1~65535) : It is used to determine the best path between devices if looping happens. Lower values will be forwarded and should be assigned to ports with fast connections. Higher values will be blocked and should be assigned to ports with slow connections. The suggestion values are 100(50~600) for 10M, 19(10~60) for 100M and 4(3~10) for 1000M connections.

Port Designated Root : This will show the root bridge ID of this segment and its bridge priority.

Port Designated Cost : This will show the path cost between the root port and the designated port of the root bridge.

Port Designated Bridge : This will show the switch’s bridge ID and its bridge priority setting.

Designated Port : This will show the port number and its port priority..

Port Forward Transitions : This is the forwarding transition counter on the port.

Port Role : It is the role of the port for the STP operation. It could be Root, Designated, Backup, or Alternated. If the port is link down, the port role will be Nonstp.

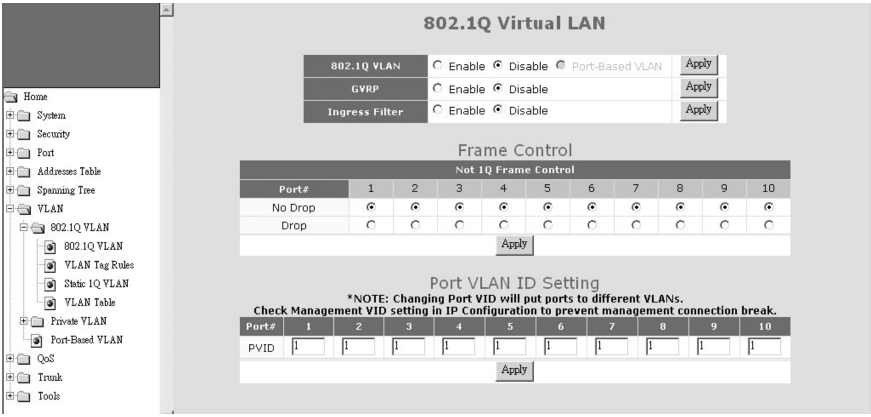
Point To Point : This is a Point-to-Point link on the port.

6.3.6 VLAN

This switch supports 802.1Q VLAN, Port-based VLAN, and Private VLAN.

1). 802.1Q VLAN

1-1). 802.1Q VLAN



802.1Q Virtual LAN

802.1Q VLAN	○ Enable ● Disable ○ Port-Based VLAN	Apply
GVRP	○ Enable ● Disable	Apply
Ingress Filter	○ Enable ● Disable	Apply

Frame Control

Not 1Q Frame Control										
Port#	1	2	3	4	5	6	7	8	9	10
No Drop	●	●	●	●	●	●	●	●	●	●
Drop	○	○	○	○	○	○	○	○	○	○

Apply

Port VLAN ID Setting

*NOTE: Changing Port VID will put ports to different VLANs.
Check Management VID setting in IP Configuration to prevent management connection break.

Port#	1	2	3	4	5	6	7	8	9	10
PVID	1	1	1	1	1	1	1	1	1	1

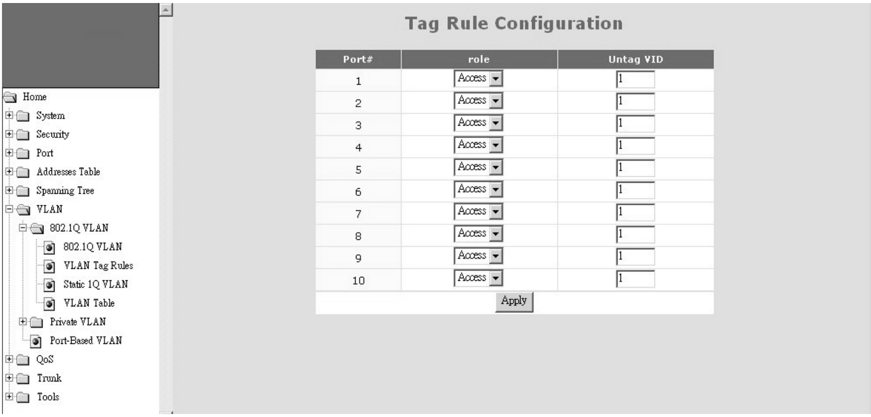
Apply

802.1Q VLAN : This is used to enable/disable 802.1Q VLAN function.
GVRP : The GVRP protocol can learn remote 802.1Q VLAN on other switches and add to dynamic 802.1Q VLAN table. You can enable/disable the operation of this protocol.
Ingress Filter : This is used to enable/disable doing VLAN filtering function at ingress port. If it is enable, the ingress port must be in the same VLAN for packet forwarding. If it is disable, VLAN filtering function will be done at egress port.

[Frame Control]
This function could be used to drop non-802.1Q frames (untagged packets).

[Port VLAN ID Setting]
PVID is used to set Port VLAN ID. When untagged packet is received, PVID of the ingress port will be used as the its VLAN ID. PVID is also used as the VLAN ID for tag adding when untagged packet is translated to tagged packet.

1-2).VLAN Tag Rules



Tag Rule Configuration

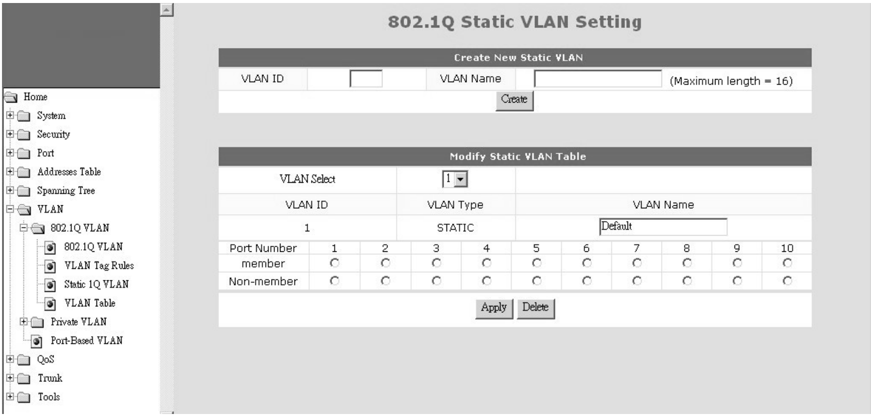
Port#	role	Untag VID
1	Access	1
2	Access	1
3	Access	1
4	Access	1
5	Access	1
6	Access	1
7	Access	1
8	Access	1
9	Access	1
10	Access	1

For 802.1Q VLAN, every port could be tag port or untag port.
Tag port will always send tagged packets and is used for switch-to-switch cascading. It is a VLAN trunk connection because there could be more than one VLAN working through it. And its role is a "**Trunk**" for 802.1Q VLAN groups operation between switches.
Untag port will always send untagged packets and is used for switch to users connection. And its role is a "**Access**" connection for users.

You can define ports as "Trunk" or "Access" according to their connection devices.

If a port is defined as "**Hybrid**", it is a tag port basically. But it will act as an untag port for packets working in VLAN defined in "Untag VID". So, it is called a hybrid port.
For example, set Port 5 as "Hybrid" and its Untag VID as 10. Port 5 will act as a tag port for all packets except packets for VLAN 10. Port 5 will act as an untag port for packets working for VLAN 10.

1-3). Static 1Q VLAN



802.1Q Static VLAN Setting

Create New Static VLAN

VLAN ID		VLAN Name	(Maximum length = 16)

Modify Static VLAN Table

VLAN Select: 1

VLAN ID	VLAN Type	VLAN Name
1	STATIC	Default

Port Number	1	2	3	4	5	6	7	8	9	10
member	○	○	○	○	○	○	○	○	○	○
Non-member	○	○	○	○	○	○	○	○	○	○

This function is used to maintain 802.1Q static VLAN.

Create an 802.1Q VLAN:

1. Input the VLAN ID and VLAN Name in “Create New Static VLAN”. Click [Create] to create the VLAN. The valid VLAN ID is 1 ~ 4094.
2. Select the VLAN in “Modify Static VLAN Table”. The new VLAN is empty by default. You can select ports for the VLAN. After that, click [Apply] to complete the VLAN configuration.

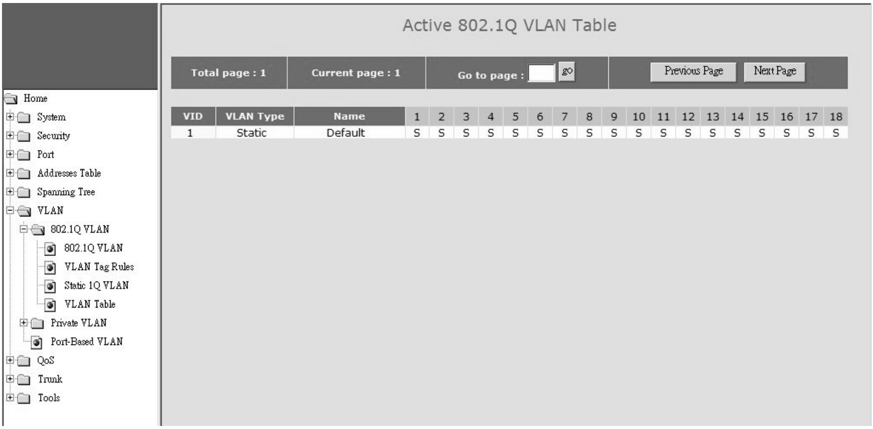
Modify an 802.1Q VLAN:

1. Select the VLAN in “Modify Static VLAN Table”.
2. Modify its setting and click [Apply] to activate the new setting.

Delete an 802.1Q VLAN:

1. Select the VLAN in “Modify Static VLAN Table”.
2. Click [Delete] to delete the 802.1Q VLAN.

1-4). VLAN Table



Active 802.1Q VLAN Table

VID	VLAN Type	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Static	Default	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

This table will show the activity of 802.1Q VLAN. Both static and dynamic 802.1Q VLAN will be shown in the table.

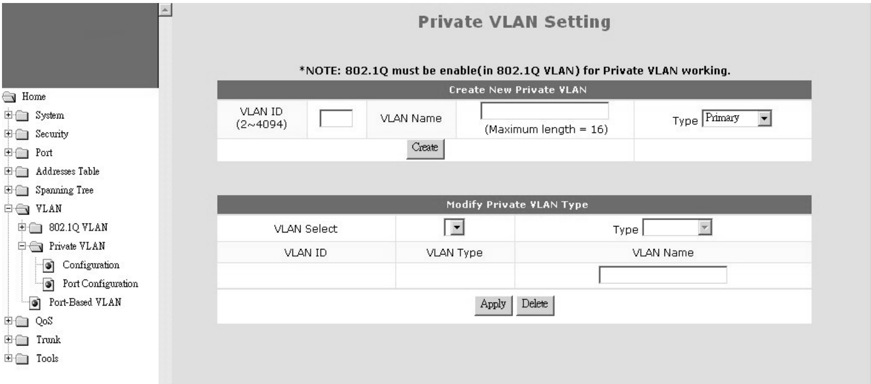
For ports, “S” means static member and “D” means dynamic member.

If GVRP protocol is enabled, this table will also show the learned remote 802.1Q VLAN.

2). Private VLAN

Three kinds of VLAN are defined for this application – Primary VLAN, Community VLAN, and Isolated VLAN. Community VLAN and Isolated VLAN can communicate with Primary VLAN, but they cannot communicate with each other. And users in Isolated VLAN cannot communicate with each other. This is a special VLAN configuration.

2-1). Configuration



Private VLAN Setting

*NOTE: 802.1Q must be enable(in 802.1Q VLAN) for Private VLAN working.

Create New Private VLAN

VLAN ID (2~4094)		VLAN Name	(Maximum length = 16)	Type Primary

Create

Modify Private VLAN Type

VLAN Select		Type
VLAN ID	VLAN Type	VLAN Name

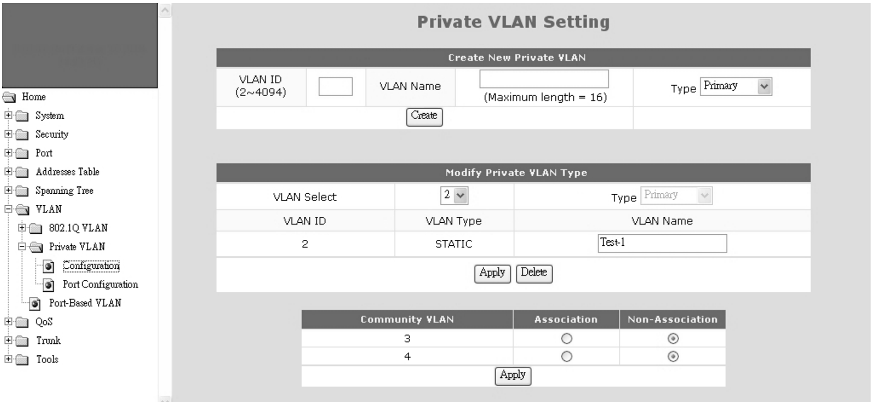
Apply Delete

Creating Private VLAN, do the steps first.

a. Create VLAN groups, and define as “Primary”, “Community”, or “Isolated”.

b. Associate Community VLAN with Primary VLAN. If more than one Primary VLAN, select Primary VLAN first and then do the association.

See the following picture.



Private VLAN Setting

Create New Private VLAN

VLAN ID (2~4094)		VLAN Name	(Maximum length = 16)	Type Primary

Create

Modify Private VLAN Type

VLAN Select	2	Type Primary
VLAN ID	VLAN Type	VLAN Name
2	STATIC	Test-1

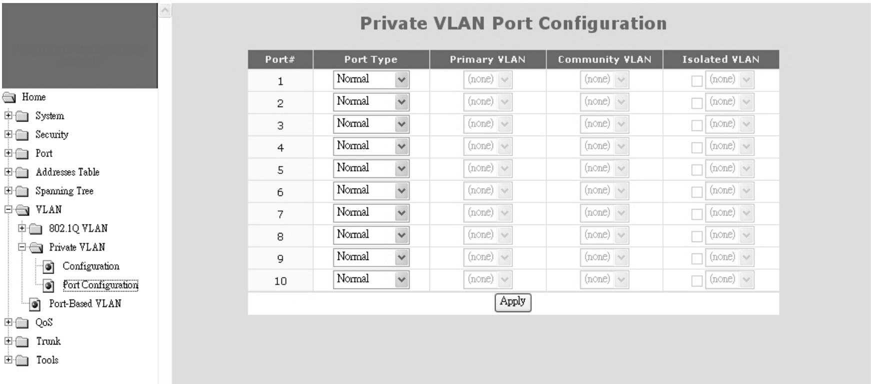
Apply Delete

Community VLAN	Association	Non-Association
3	○	◉
4	○	◉

Apply

2-2). Port Configuration

After VLANs are created, assign ports to VLANs.



Private VLAN Port Configuration

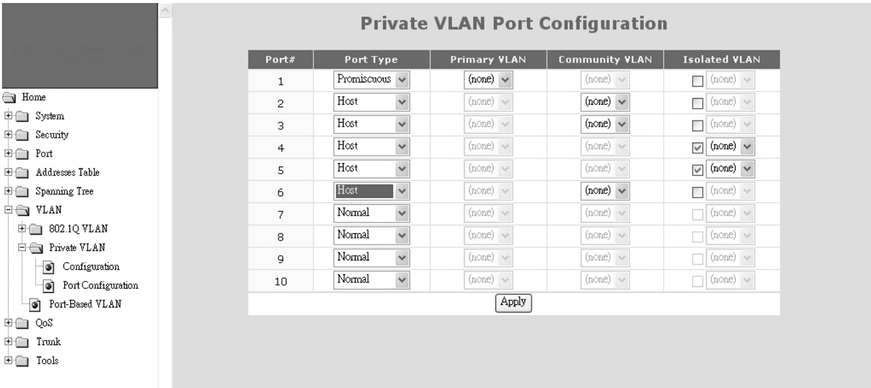
Port#	Port Type	Primary VLAN	Community VLAN	Isolated VLAN
1	Normal	(none)	(none)	□ (none)
2	Normal	(none)	(none)	□ (none)
3	Normal	(none)	(none)	□ (none)
4	Normal	(none)	(none)	□ (none)
5	Normal	(none)	(none)	□ (none)
6	Normal	(none)	(none)	□ (none)
7	Normal	(none)	(none)	□ (none)
8	Normal	(none)	(none)	□ (none)
9	Normal	(none)	(none)	□ (none)
10	Normal	(none)	(none)	□ (none)

There are three types for a port - Normal, Host, and Promiscuous.
“Normal” is for ports doing normal operation instead of Private VLAN.
“Host” is for ports that could be in Community VLAN or Isolated VLAN.
“Promiscuous” is for ports that could be in Primary VLAN or Isolated VLAN.

Follow the steps to do the port assignment.

a. Select the type for a port.
b. If it is “Host”, you can select a VLAN from Community VLAN or mark Isolated VLAN and select from it.
c. If it is “Promiscuous”, you can select a VLAN from Primary VLAN or mark Isolated VLAN and select from it.
d. Repeat a.~c. to complete the port assigment.
e. Click [Apply].

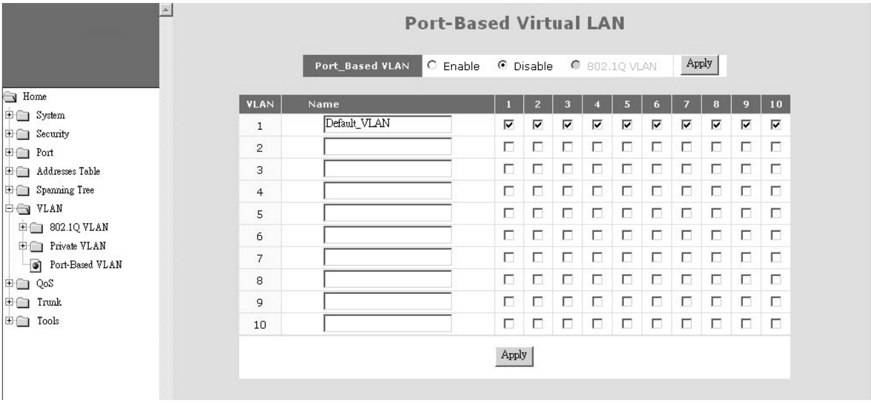
Please see the following picture.



Private VLAN Port Configuration

Port#	Port Type	Primary VLAN	Community VLAN	Isolated VLAN
1	Promiscuous	(none)	(none)	□ (none)
2	Host	(none)	(none)	□ (none)
3	Host	(none)	(none)	□ (none)
4	Host	(none)	(none)	☑ (none)
5	Host	(none)	(none)	☑ (none)
6	Host	(none)	(none)	□ (none)
7	Normal	(none)	(none)	□ (none)
8	Normal	(none)	(none)	□ (none)
9	Normal	(none)	(none)	□ (none)
10	Normal	(none)	(none)	□ (none)

3). Port-based VLAN



Port-Based Virtual LAN

Port_Based VLAN ○ Enable ● Disable ○ 802.1Q VLAN [Apply]

VLAN	Name	1	2	3	4	5	6	7	8	9	10
1	Default_VLAN	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2		□	□	□	□	□	□	□	□	□	□
3		□	□	□	□	□	□	□	□	□	□
4		□	□	□	□	□	□	□	□	□	□
5		□	□	□	□	□	□	□	□	□	□
6		□	□	□	□	□	□	□	□	□	□
7		□	□	□	□	□	□	□	□	□	□
8		□	□	□	□	□	□	□	□	□	□
9		□	□	□	□	□	□	□	□	□	□
10		□	□	□	□	□	□	□	□	□	□

[Apply]

Follow the steps to configure Port-based VLAN.

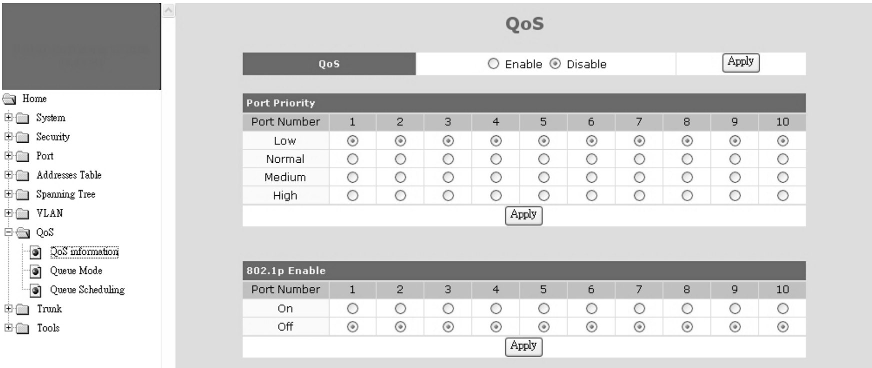
a. Enable Port-based VLAN. And click [Apply] button.
b. Give VLAN name.
c. Select ports for each VLAN.
d. Click [Apply] button.

6.3.7 QoS

This switch supports Port-based priority, 802.1P priority, and DSCP priority. These priority operations could be enable/disable on each port.

For 802.1P and DSCP priority operations, their priority values can be mapped to four priority queues of the switch for QoS operation.

1). QoS Information



QoS

QoS	○ Enable ● Disable	Apply

Port Priority										
Port Number	1	2	3	4	5	6	7	8	9	10
Low	●	●	●	●	●	●	●	●	●	●
Normal	○	○	○	○	○	○	○	○	○	○
Medium	○	○	○	○	○	○	○	○	○	○
High	○	○	○	○	○	○	○	○	○	○

Apply

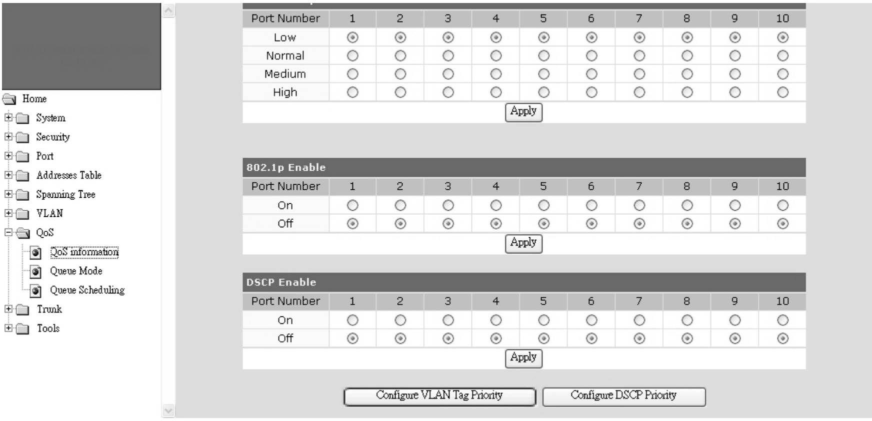
802.1p Enable										
Port Number	1	2	3	4	5	6	7	8	9	10
On	○	○	○	○	○	○	○	○	○	○
Off	●	●	●	●	●	●	●	●	●	●

Apply

QoS : this is for QoS function enable/disable.
Port Priority : this is used to define the priority setting of each port. It will map to the four priority queues of the switch.
802.1P Enable : this is for 802.1P priority operation enable/diable on each port. 802.1P priority operation will use the priority setting in tag of packets for QoS operation.
The mapping of 802.1P priority values (0~7) to priority queue could be defined at "VLAN Tag Priority" page by clicking [Configure VLAN Tag Priority] button.
DSCP Enable : (see the following picture) this is for DSCP(Differential Service Code Point) priority operation enable/disable on each port. DSCP priority operation will use the priority setting in ToS field of IP packets for QoS operation.
Seven DSCP values (0~63) could be defined and map to priority queue at "IP Differential Service (DiffServ) Configuration" page by clicking [Configure DSCP Priority] button.

[Configure VLAN Tag Priority] button : Click this button can go to the "VLAN Tag Priority" page for 802.1P priority values (0~7) to priority queue mapping setting.

[Configure DSCP Priority] button : Click this button can go to the "IP Differential Service (DiffServ) Configuration" page for DSCP priority values (0~63) to priority queue mapping setting.



Port Number	1	2	3	4	5	6	7	8	9	10
Low	●	●	●	●	●	●	●	●	●	●
Normal	○	○	○	○	○	○	○	○	○	○
Medium	○	○	○	○	○	○	○	○	○	○
High	○	○	○	○	○	○	○	○	○	○

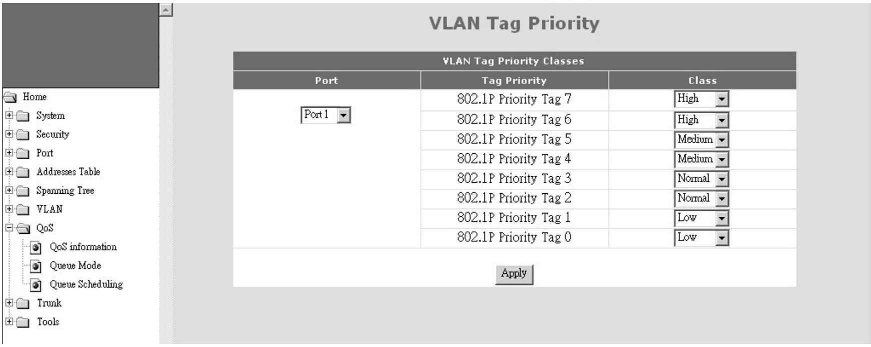
802.1p Enable

Port Number	1	2	3	4	5	6	7	8	9	10
On	○	○	○	○	○	○	○	○	○	○
Off	●	●	●	●	●	●	●	●	●	●

DSCP Enable

Port Number	1	2	3	4	5	6	7	8	9	10
On	○	○	○	○	○	○	○	○	○	○
Off	●	●	●	●	●	●	●	●	●	●

[802.1P Priority Mapping]



VLAN Tag Priority

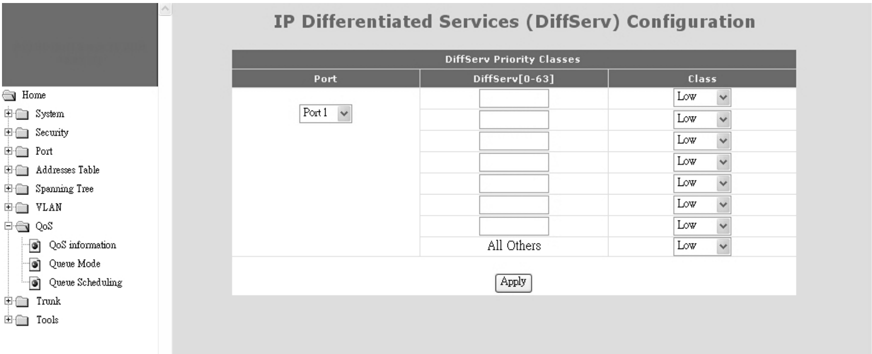
VLAN Tag Priority Classes

Port	Tag Priority	Class
Port 1	802.1P Priority Tag 7	High
	802.1P Priority Tag 6	High
	802.1P Priority Tag 5	Medium
	802.1P Priority Tag 4	Medium
	802.1P Priority Tag 3	Normal
	802.1P Priority Tag 2	Normal
	802.1P Priority Tag 1	Low
	802.1P Priority Tag 0	Low

For 802.1P priority, priority value (0~7) in VLAN tag will be used for QoS operation. And the mapping of priority values to priority queues (High/Middle /Normal/Low) could be defined here.

If 802.1P priority function is enabled, these settings will be followed for QoS operation.

[DiffServ Priority Mapping]

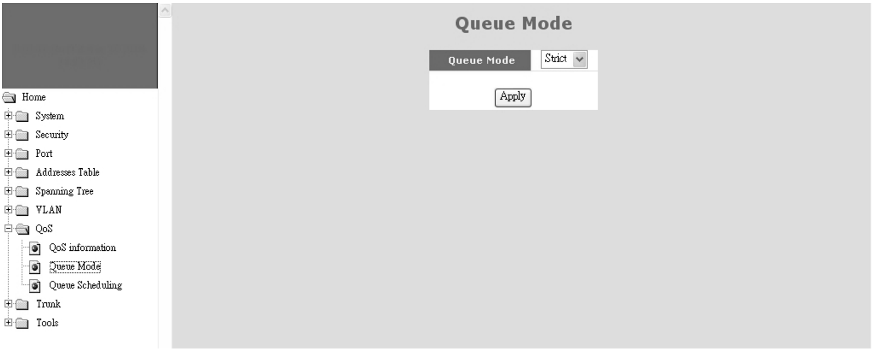

IP Differentiated Services (DiffServ) Configuration

DiffServ Priority Classes		
Port	DiffServ[0-63]	Class
Port 1		Low
		Low
		Low
		Low
		Low
		Low
		Low
	All Others	Low

DSCP priority operation will use the priority setting in ToS field of IP packets for QoS operation.
Seven DSCP values (0~63) could be defined and map to priority queues (High /Middle/Normal/Low).

If DSCP priority function is enabled, these settings will be followed for QoS operation.

2). Queue Mode


Queue Mode

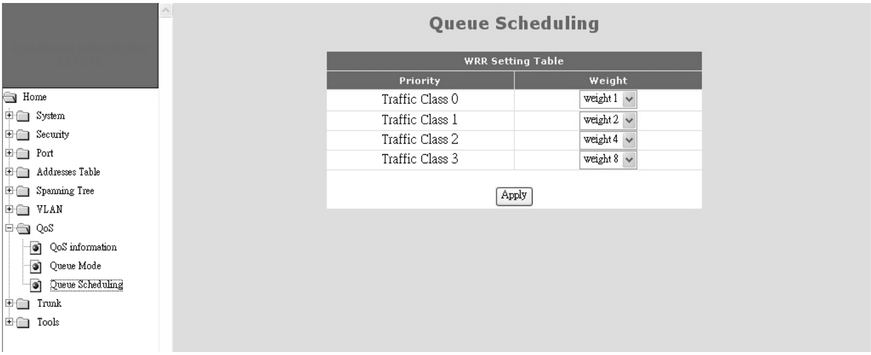
Queue Mode: Strict

This switch supports Strict Priority and WRR (Weight Round Robin) operation for sending out packets from piority queues.

If Strict Priority is selected, packets in higher priority queues will always get bandwidth service first. Lower priority queues will get service when higher priority queues are empty.

If WRR is selected, priority queues will be served with the weighting of priorities. And the setting of weight could be configured at “Queue Scheduling”.

3). Queue Scheduling



Queue Scheduling

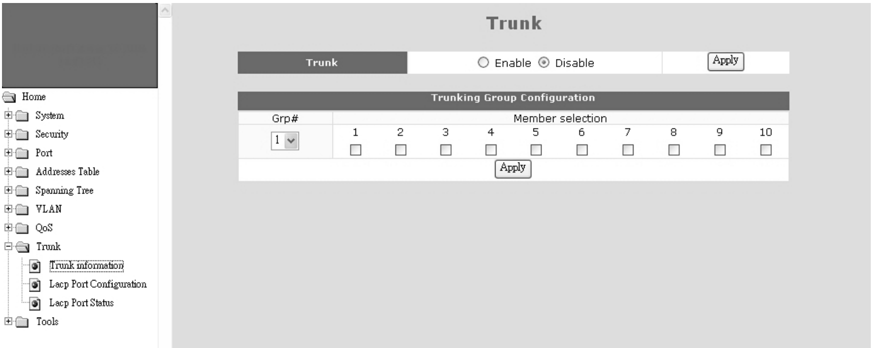
WRR Setting Table	
Priority	**Weight**
Traffic Class 0	weight 1
Traffic Class 1	weight 2
Traffic Class 2	weight 4
Traffic Class 3	weight 8

This function is used to configured the weight of priority queues for WRR operation. And the output bandwidth will be shared with the ratio of weight between priority queues.

6.3.8 Trunk

This switch supports up to eight trunk groups. And the trunk could be configured with static assigned or by LACP (Link Aggregation Control Protocol) protocol.

1). Trunk Information



Trunk

Trunk ○ Enable ● Disable Apply

Trunking Group Configuration

Grp#	Member selection									
	1	2	3	4	5	6	7	8	9	10
1	□	□	□	□	□	□	□	□	□	□

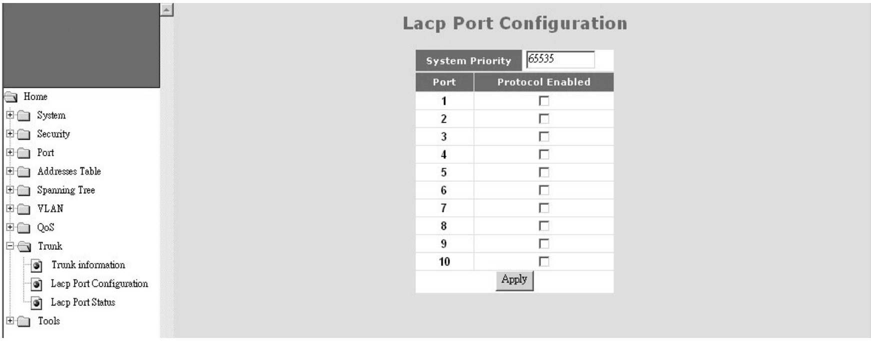
Apply

This table is used to assign ports to Trunk groups statically.

Follow the steps to do it. (*Don't connect trunk cables until this function is set.)
a. Enable Trunk function first. Then click [Apply].
b. Select a Trunk Group at "Grp#".
c. Select the member ports.
d. Click [Apply].
e. Repeat b.~d. for another Trunk group setting.

Note: If a port are used as static port for any Trunk group, its LACP function will be disable.

2). Lacp Port Configuration



Lacp Port Configuration

System Priority 65535

Port	Protocol Enabled
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□

Apply

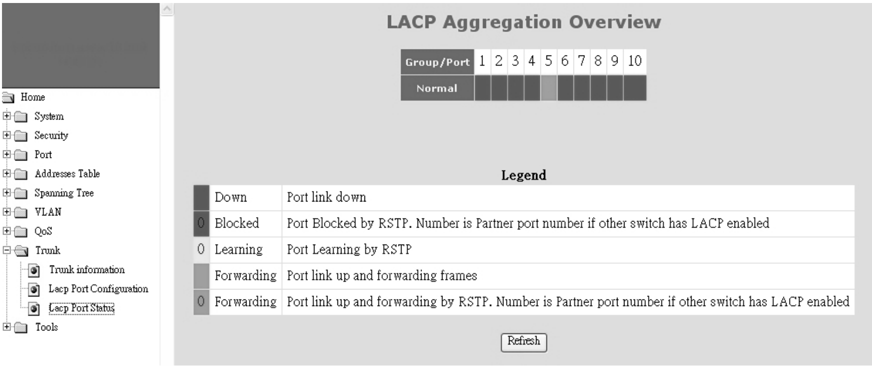
This page is used to configure LACP function. With LACP protocol, switches can learn trunk connections automatically.

Follow the steps to do it. (*Don't connect trunk cables until this function is set.)

a. Enable Trunk function at "Trunk Information" page first. Then click [Apply].
b. Assign System Priority. (Its value is 1~65535 and higher numbers have lower priority. Combining with the Mac address of the switch, it is used to identify this switch in LACP protocol operation.)
c. Select ports that will run LACP protocol.
d. Click [Apply].

Note: If ports are already in static trunk group, they are not allowed to apply as LACP ports. If static ports are selected as LACP ports, warning message will be prompted when [Apply] is clicked.

3). Lacp Port Status



LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10
Normal	■	■	■	■	▨	■	■	■	■	■

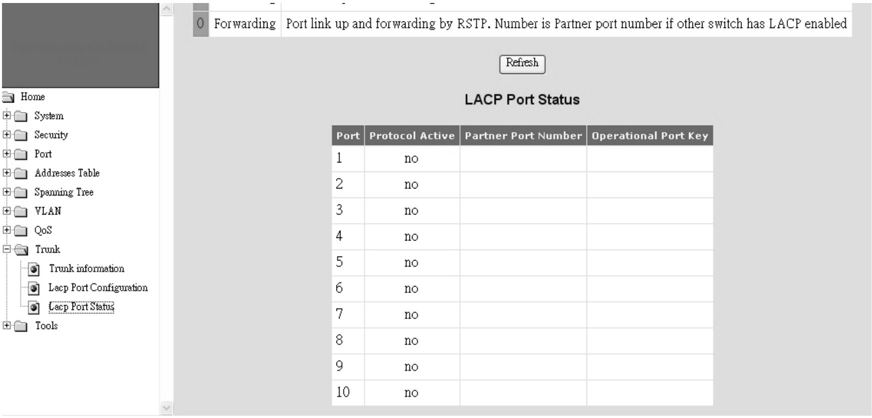
Legend

■	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
▨	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

This is for LACP protocol running status.

You can see current port status with colors. If LACP trunk is created, another port groups message will be shown.
Click [Refresh] can update the status information.

The following table will show the LACP enable/disable status of each port. And the port number and port key of the partner switch will also be shown in the table when LACP Trunk is running.



0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

LACP Port Status

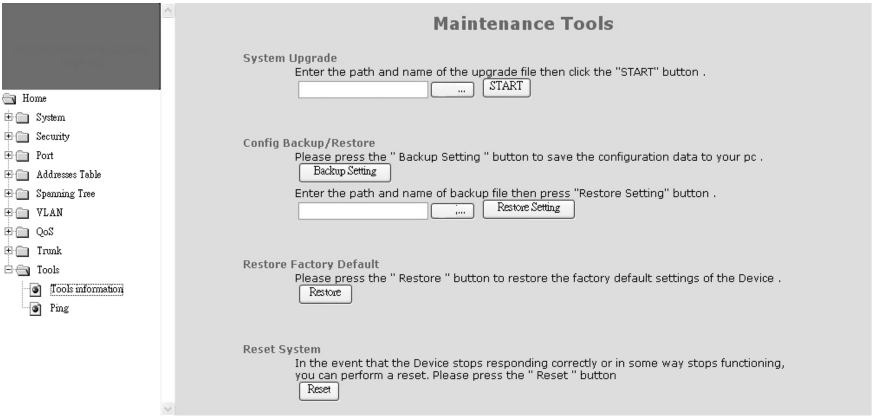
Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	no		
8	no		
9	no		
10	no		

6.3.9 Tools

The follow functions are used for system maintenance. They are Software Upgrade, Configuration Backup/Restore, Restore Factory Default, Reset System, and Ping functions.

1). Tools Information

Four functions are supported as the system maintenance tools.



Maintenance Tools

System Upgrade

Enter the path and name of the upgrade file then click the "START" button .

Config Backup/Restore

Please press the " Backup Setting " button to save the configuration data to your pc .

Enter the path and name of backup file then press "Restore Setting" button .

Restore Factory Default

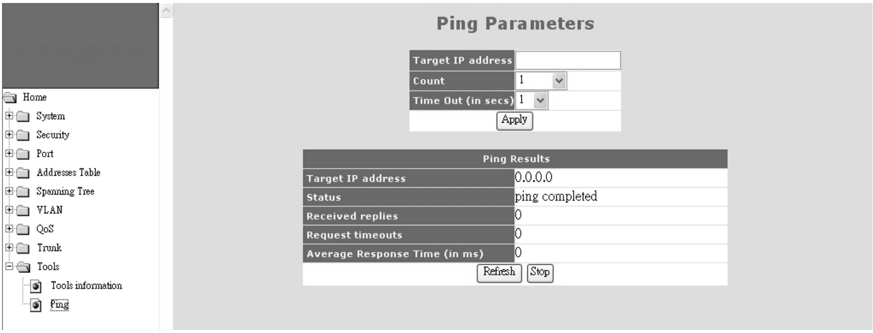
Please press the " Restore " button to restore the factory default settings of the Device .

Reset System

In the event that the Device stops responding correctly or in some way stops functioning, you can perform a reset. Please press the " Reset " button

System Upgrade : This function will upgrade the system operation software from the web management PC.
Config Backup/Restore : Clicking [Backup Setting] button, the switch can backup the configuration of the switch to the web management PC.
And the configuration of the switch can be restored to switch by [Restore Setting] button after the configuration file is selected.
Restore Factory Default : This function will restore the switch configuration to factory default setting.
Reset System : This function will cause the switch to reboot itself.

2). Ping



Ping Parameters

Target IP address	
Count	1
Time Out (in secs)	1

Ping Results	
Target IP address	0.0.0.0
Status	ping completed
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

This function is used to ping network devices from the switch. It can be used to verify network connection.

Target IP address : This is the target IP address for the ping operation.
Count : This is the repeat count for the ping operation.
Time Out : This is the timeout value for the ping operation.
After the above items are set, click [Apply] to start the ping operation.

Then the result of ping operation will be shown.

7. Software Update and Backup

This switch supports software update and configuration backup/update/restore functions. It could be done in two ways.

1. **From console when booting**: by Xmodem protocol and doing by terminal program. This function can be used for run-time code and boot code updating. (Boot code works only at boot time - before the main program starts.)

   Press Ctrl-C when the switch is booting, the following message will be shown.

   ```
           Boot Menu
   ===========================
   0: Start the Run-time code
   1: Upgrade Run-time code
   2: Upgrade Boot Code

   => Select:
   ```

   a. *Start Run-time code* : This option will continue the booting process.

   b. *Upgrade Run-time code* : This option will try to update run-time code (main code) from terminal program with Xmodem protocol. If this option is selected, the following message will be shown.
   "Waiting to receive file by Xmodem ...."
   Then user can select "Send File" function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

   c. *Upgrade Boot Code* : This option will try to update boot code from terminal program with Xmodem protocol. User can select "Send File" function of terminal program and select Xmodem protocol and the update file, then start the file upgrade.

2. **From web browser**: Doing by http protocol and by web browser. Please refer to the description of "*Tools*" function in Section 6.3.

A. Product Specifications

[8TX+2SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each TX port
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M), FDX/Col.
Number of Ports	8* RJ45 TX, 2* SFP ports (10 GE Ports totally)
Dimensions	250 x 117 x 37 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	802.1Q VLAN, Port-based VLAN, Private VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/DSCP priority operation
Spanning Tree	Support RSTP/STP protocol
Trunking	8 groups max., Static and LACP are supported
Mirror Port	Yes
Mac ID Security on Port	Static Mac address access limit on port, and Dynamic Mac address number limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 128Kbps~1000Mbps, for ingress/egress traffic
Storm Control	Broadcast, Multicast, and Unicast Storm Control
Admin Manage Security	Yes, by IP/Subnet/Interface limit
System Time	Yes, by NTP protocol
System Log	Yes, Local and Remote (by syslog) logging
Out-band Management	Console (basic settings only)
In-band Management	http
Software Update/Backup	by http protocol, Xmodem, for firmware/ configuration

[16TX+4SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each TX port
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M), FDX/Col.
Number of Ports	16* RJ45 TX, 4* SFP(shared) ports (16 GE Ports totally)
Dimensions	440 x 172 x 43 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	802.1Q VLAN, Port-based VLAN, Private VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/DSCP priority operation
Spanning Tree	Support RSTP/STP protocol
Trunking	8 groups max., Static and LACP are supported
Mirror Port	Yes
Mac ID Security on Port	Static Mac address access limit on port, and Dynamic Mac address number limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 128Kbps~1000Mbps, for ingress/egress traffic
Storm Control	Broadcast, Multicast, and Unicast Storm Control
Admin Manage Security	Yes, by IP/Subnet/Interface limit
System Time	Yes, by NTP protocol
System Log	Yes, Local and Remote (by syslog) logging
Out-band Management	Console (basic settings only)
In-band Management	http
Software Update/Backup	by http protocol, Xmodem, for firmware/ configuration

[24TX+4SFP Model]

Access Method	Ethernet, CSMA/CD
Standards Conformance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE IEEE 802.3z, IEEE 802.3ab (1000Base)
Communication Rate	10/100/1000Mbps, Full / Half duplex (auto-negotiation)
MDI/MDIX	Auto-detect for each TX port
Indicator Panel	LEDs for each unit : Power, System each port : Link/Act(Green:1000M, Yellow:10/100M), FDX/Col.
Number of Ports	24* RJ45 TX, 4* SFP(shared) ports (24 GE Ports totally)
Dimensions	440 x 172 x 43 mm
Certification	CE Mark, FCC Class A
Temperature	Standard Operating: 0 to 50℃
Humidity	10% to 90% (Non-condensing)
Bridging Function	Filtering, forwarding and learning
Switching Method	Store-and-forward
Address Table	8K entries
Filtering/Forwarding Rate	Line speed
Maximum Packet Size	9600 Bytes
Flow Control	802.3x for full duplex, backpressure for half duplex
VLAN	802.1Q VLAN, Port-based VLAN, Private VLAN
QoS	4 transmit priorities per ports, for port-based/802.1P tagged-based/DSCP priority operation
Spanning Tree	Support RSTP/STP protocol
Trunking	8 groups max., Static and LACP are supported
Mirror Port	Yes
Mac ID Security on Port	Static Mac address access limit on port, and Dynamic Mac address number limit on port
802.1x	Yes, support Authentication and Transparent modes
Rate Control	Yes, 128Kbps~1000Mbps, for ingress/egress traffic
Storm Control	Broadcast, Multicast, and Unicast Storm Control
Admin Manage Security	Yes, by IP/Subnet/Interface limit
System Time	Yes, by NTP protocol
System Log	Yes, Local and Remote (by syslog) logging
Out-band Management	Console (basic settings only)
In-band Management	http
Software Update/Backup	by http protocol, Xmodem, for firmware/ configuration

B. Compliances

EMI Certification FCC Class A Certification (USA)

Warning: This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A digital device pursuant to Subpart B of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are required to correct the interference.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014. It conforms to the following specifications:

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4kV CD, 8kV AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1kV - (power line), 0.5kV - (signal line)

This product complies with the requirements of the Low Voltage Directive 2006/95/EC and the EMC Directive 2004/108/EC.

Warning! Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

C. Warranty

We warrant to the original owner that the product delivered in this package will be free from defects in material and workmanship for a period of warranty time from the date of purchase from us or the authorized reseller. The warranty does not cover the product if it is damaged in the process of being installed. We recommend that you have the company from whom you purchased this product install it.